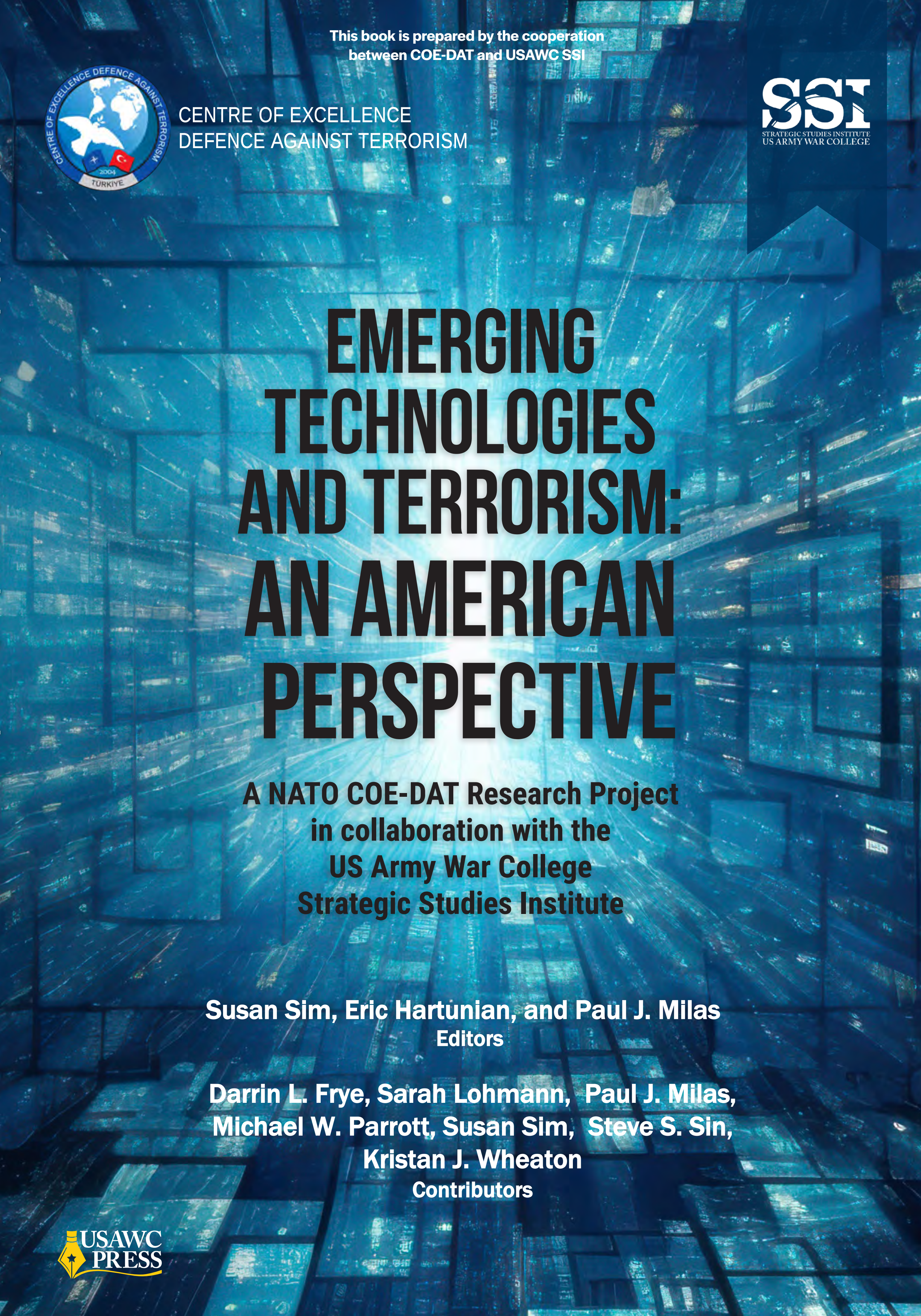


This book is prepared by the cooperation
between COE-DAT and USAWC SSI

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

SSI
STRATEGIC STUDIES INSTITUTE
US ARMY WAR COLLEGE

EMERGING TECHNOLOGIES AND TERRORISM: AN AMERICAN PERSPECTIVE

A NATO COE-DAT Research Project in collaboration with the US Army War College Strategic Studies Institute

Susan Sim, Eric Hartunian, and Paul J. Milas
Editors

Darrin L. Frye, Sarah Lohmann, Paul J. Milas,
Michael W. Parrott, Susan Sim, Steve S. Sin,
Kristan J. Wheaton
Contributors

USAWC PRESS

STRATEGIC STUDIES INSTITUTE
US ARMY WAR COLLEGE

“The Army’s Think Tank”

The Strategic Studies Institute (SSI) is the US Army’s institute for geostrategic and national security research and analysis. SSI research and analysis creates and advances knowledge to influence solutions for national security problems facing the Army and the nation.

SSI serves as a valuable source of ideas, criticism, innovative approaches, and independent analyses as well as a venue to expose external audiences to the US Army’s contributions to the nation. It acts as a bridge to the broader international community of security scholars and practitioners.

SSI is composed of civilian research professors, uniformed military officers, and a professional support staff, all with extensive credentials and experience. SSI’s Strategic Research and Analysis Department focuses on global, transregional, and functional security issues. Its Strategic Engagement Program creates and sustains partnerships with strategic analysts around the world, including the foremost thinkers in the field of security and military strategy. In most years, about half of SSI’s publications are written by these external partners.

Research Focus Arenas

Geostrategic net assessment—regional and transregional threat analysis, drivers of adversary conduct, interoperability between partner, allied, IA, commercial, and Joint organizations

Geostrategic forecasting—geopolitics, geoeconomics, technological development, and disruption and innovation

Applied strategic art—warfare and warfighting functions, Joint and multinational campaigning, and spectrum of conflict

Industrial/enterprise management, leadership, and innovation—ethics and the profession, organizational culture and effectiveness, transformational change, talent development and management, and force mobilization and modernization

Emerging Technologies and Terrorism: An American Perspective

A NATO COE-DAT Research Project in Collaboration with the US Army War College Strategic Studies Institute

Susan Sim, Eric Hartunian, and Paul J. Milas
Editors

Darrin L. Frye, Sarah Lohmann, Paul J. Milas,
Michael W. Parrott, Susan Sim, Steve S. Sin,
Kristan J. Wheaton
Contributors

April 2024

USAWC PRESS
US ARMY WAR COLLEGE
Strategic Studies Institute

The views expressed in this publication are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, the US government, or NATO COE-DAT. Authors of Strategic Studies Institute and US Army War College Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official US policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is cleared for public release; distribution is unlimited.

******

******

Comments pertaining to this publication are invited and should be forwarded to: Director, Strategic Studies Institute and US Army War College Press, US Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5244.

******

ISBN 1-58487-853-3

Cover Image Credits

The cover was designed using assets from Freepik.

Image description: Global business internet network connection iot internet of things business intelligence concept busines global network, https://www.freepik.com/free-photo/global-business-internet-network-connection-iot-internet-things-business-intelligence-concept-busines-global-network-futuristic-technology-background-ai-generative_49395782.htm

Image by: benzoix on Freepik

Table of Contents

Preface

This project builds upon the foundation laid by NATO's Centre of Excellence Defence Against Terrorism (COE-DAT) 2022 research endeavor conducted in collaboration with TOBB University of Economics and Technology, a university based in Ankara, Türkiye, that explored the research question: "What are the emerging future threats in the future from an Asian, African, and European perspective?"

In continuation of this effort, the current project shifts focus to North America and South America, focusing on emerging disruptive technologies over the next five to 10 years. By expanding the regional scope, the study provides a comprehensive understanding of emerging threats posed by terrorists within the North and South American continents. This project builds on the insights gained from the previous research. It identifies and analyzes the evolving landscape of terrorism in North and South America through the lens of emerging disruptive technologies.

Understanding the threats posed by terrorists and terrorist groups in the context of emerging disruptive technologies is essential for enhancing national and international security in an increasingly complex and interconnected world. The project, therefore, contributes valuable insights to inform policy formulation, enhance security measures, and foster international cooperation in countering terrorism within the region, which is imminent for multiple reasons.

- By comprehending and identifying these potential threats, military and civilian decisionmakers and security agencies can prevent terrorist attacks by developing and implementing proactive strategies that use new technologies and mitigate the risks associated with the misuse of emerging technologies by terrorist groups. Terrorist organizations constantly adapt, innovate, and leverage emerging technologies for nefarious purposes. Security forces can maintain an advantage over their adversaries by staying informed.
- Given the global nature of terrorism, understanding emerging threats facilitates international collaboration and information sharing among nations and organizations like NATO, enhancing collective security efforts.

- Understanding the potential misuse of emerging technologies by terrorists allows policymakers to develop measures that protect national security and safeguard civil liberties and privacy rights.
- Understanding the nature of emerging threats helps planners allocate resources effectively and focus counterterrorism efforts on the most pressing issues.

The COE-DAT provides key decisionmakers with a comprehensive understanding of terrorism and counterterrorism to assist them with the transformation efforts of NATO and nations of interest to meet future challenges. This transformation is embedded in NATO's three core tasks: deterrence and defense, crisis prevention and management, and cooperative security.

As a strategic think tank focused on developing NATO DAT activities outside NATO's command and force structure, COE-DAT supports NATO's long-term military transformation by anticipating and preparing for the ambiguous, complex, and rapidly changing future security environment. The center supports academic freedom and interacts with universities, think tanks, researchers, international organizations, and global partners to provide critical thought on the sensitive topic of counterterrorism and increases information sharing within NATO and with NATO's partners to ensure the retention and application of acquired experience and knowledge.

The US Army War College Strategic Studies Institute, the US Army's premier strategic-level think tank, conducts independent, multidisciplinary research and analysis on international security, geostrategic, and other topics for the US Department of Defense and the broader national security and interagency communities. Its successful partnership with COE-DAT allows both organizations to collaborate and develop timely research, analysis, and education on security issues for NATO, its Allies, and partner nations.

Bülent Akdeniz
Colonel (Türkiye Army)
Director, COE-DAT
February 2024

Acknowledgments

Emerging disruptive technologies, when in the wrong hands, pose a significant risk to the security of modern societies. The importance of addressing emerging disruptive technologies in the context of national security cannot be overstated. As we navigate this dynamic landscape, it is imperative to recognize the potential threats posed when these technologies fall into the wrong hands. The misuse of such innovations by terrorists can pose a significant risk to security, making it essential to understand, anticipate, and proactively address these challenges.

This collaborative project between the United States Army War College Strategic Studies Institute (USAWC SSI) and Centre of Excellence Defence Against Terrorism (COE-DAT) serves as a vital platform for fostering a deeper understanding of the implications of emerging disruptive technologies and developing strategies to safeguard our societies against potential threats. COE-DAT is grateful for the collective effort invested in this initiative and remain committed to advancing our shared goal of enhancing national security in the face of evolving technology developments.

This collaborative effort stands as a testament to the commitment of both organizations to advancing knowledge and understanding in the realm of emerging disruptive technologies.

COE-DAT strives to be the hub of a wider network or community of interest (CoI) regarding counterterrorism for NATO. COE-DAT provides key decisionmakers a comprehensive understanding to terrorism and counterterrorism challenges, in order to transform NATO, and nations of interest to meet future security challenges. The vision and mission of COE-DAT, and the comprehensive efforts towards supporting Alliance transformations, nests with NATO's three declared core tasks of deterrence and defense, crisis prevention and management, and cooperative security.

The USAWC SSI conducts research and analysis to solve geostrategic issues for the US Army and the national security community. The emerging disruptive technologies project is another excellent collective partnership between COE-DAT and the USAWC SSI. COE-DAT extends its deepest gratitude to the USAWC SSI for their collaboration on this project, particularly to Colonel Eric Hartunian (US Army) and Lieutenant Colonel Paul J. Milas (US Army) for their invaluable leadership and contribution to making this project into a book.

Our special thanks go to the distinguished group of authors for their collaboration and exceptional efforts to make this book happen, namely Dr. Darrin Frye, Mr. Kristan Wheaton, Dr. Steve S. Sin, Dr. Sarah Lohmann, and Mr. Michael Parrott. The collective efforts of the authors have played a pivotal role in advancing our understanding of emerging disruptive technologies. Their commitment to excellence, under the leadership of the academic adviser of this project, Ms. Susan Sim, has been instrumental in shaping the insights presented in the book.

Finally, our gratitude goes to the fine staff of COE-DAT that were involved in this project in various functions. We thank Major Ali Mavuş (Türkiye Army) and Lieutenant Colonel Uwe Berger (German Army) for their work in coordinating the project with the USAWC SSI representatives. Ms. Selvi Kahraman was essential in keeping the research team connected.

Carol V. Evans

Dr. Carol V. Evans
Director, Strategic Studies Institute
and US Army War College Press

Bülent Akdeniz
Colonel (Türkiye Army)
Director, COE-DAT

Executive Summary

The weaponization of new technologies by non-state actors has long been of concern to policymakers. Although recent advances in artificial intelligence (AI) and autonomous systems promise to facilitate the early detection and prevention of terrorist threats, terrorist groups and violent extremists are already exploiting these technologies to mobilize, plan, and carry out attacks.

Now, with futurists promising AI will soon be everywhere, nature and human genes becoming editable, parts of the metaverse becoming real, and technology bridging the digital and physical worlds, how might emerging technologies change the terrorist landscape in the next five to 10 years?

To examine the key threats terrorism experts assess to be facing North America and South America in relation to emerging technologies, the NATO Centre of Excellence Defence Against Terrorism (COE-DAT)'s emerging threats in terrorism project partnered with the US Army War College Strategic Studies Institute to produce this report. Over several months in 2023, the institute conducted two workshops that brought together experts in nanoweaponry, cybersecurity and AI, augmented reality, and biosecurity who are on the front lines of terrorist threat assessment and operational response.

The institute asked participants to forecast possible threat scenarios involving emerging technologies—innovative technologies that have been recently developed, are under development, or are likely to be developed in the next few years—and to recommend countermeasures and mitigation strategies. The experts' findings include the following.

- The terrorist AI toolbox includes technologies such as ChatGPT, drones, and biometrics. Terror groups are already using these tools for recruitment, warfare, and the hacking of high-value systems. Terrorists have also practiced using automated vehicles for targeted attacks and loss of life. Experts expect the malicious use of AI, including the creation of deepfake videos to sow disinformation to polarize societies and deepen grievances, to grow over the next decade.

- Within the next decade, the probability is high that violent extremist organizations will leverage technological advancements in the agricultural industry to cause catastrophic attacks that increase food insecurity and result in economic loss. Globalization will exacerbate the impacts of these attacks due to interdependence between the world's economies and the agricultural sector.
- Over the next five to 10 years, augmented reality tools will present unique opportunities for collaboration that terrorist networks will likely exploit to operate easily across borders. Technologies like smart glasses will allow users to overlay two-dimensional and three-dimensional digital images onto the real-world environment. This augmentation could enable terrorists to "travel" to foreign countries, allowing them to meet with collaborators in emotionally impactful and nearly physical ways without needing proper documentation.
- With more countries developing biomedical and biotechnological capacities in response to the logistical challenges the countries experienced during the COVID-19 pandemic, barriers to access and training standards for handling hazardous material properly have been lowered. Therefore, the risk of bad actors acquiring and producing at scale more diversified and sophisticated biological materials has increased.
- The study of ultrasmall nanotechnology has ushered in a new era of scientific development that could allow nefarious actors to manipulate nanomolecular properties to craft tiny yet highly destructive instruments that pose grave threats to humanity. The size, low cost, scalability, and targeting precision of such nanoweapons will make them ideal for covert attack. Terrorists with access to nanoweaponry will have the opportunity to threaten entities that have enjoyed relative immunity to traditional modes and past methods of terrorism.

When these threat scenarios were presented at the NATO COE-DAT's flagship Terrorism Experts Conference in Ankara in October 2023, a key question posed was whether this study is an exercise in pondering the improbable.

Although some of the scenarios discussed in this report can be extrapolated from past data and terrorist manifestos, other scenarios may appear to have been drawn from Hollywood movies. So, is life imitating art? In an era in which the transformative power of emerging technologies is everywhere, all at once, the line separating fiction from reality is blurring. Previous studies have suggested terrorist groups are motivated to innovate and seek new technologies, targets, and opportunities to overcome tactical problems such as security measures or logistical challenges. The increasingly prevalent use of drones to attack well-protected and long-distance targets is one example.

Emerging technologies also have a democratizing effect. Whereas in the past, only larger, resource-rich terrorist organizations could afford to innovate, the increasing accessibility and affordability of new technologies mean even small extremist cells can now carry out mass casualty attacks by, for instance, hacking into the Internet of Things to turn unmanned vehicles into smart bombs from the safety of distance and anonymity.

Can one rule out devious plots to wipe out specific groups of people or to cause food shortages in the Americas when the technology to do so is available? Families in Indonesia have perpetrated suicide bombings, sacrificing their children in the process, because the families believed the end of time was near. What would stop terrorist groups with apocalyptic worldviews or millenarian beliefs from seeking to fulfill their own prophecies of famine, drought, and genocide?

The current thinking of the US intelligence community is, although most terrorist attacks will continue to use small arms and improvised explosives for the foreseeable future because these means are sufficient and reliable, terrorists will also seize any opportunity to develop new, more remote attack methods—especially novel weapons of mass destruction that will allow bad actors to conduct spectacular mass casualty attacks.

Recommendations for NATO

The *NATO 2022 Strategic Concept* recognizes emerging and disruptive technologies bring both opportunities and risks, alter the character of conflict, and become key arenas of global competition. Thus, NATO seeks to retain its strategic and effective dominance in nine priority technology areas: AI, autonomous systems, quantum-enabled technologies, biotechnologies and human enhancement, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, and next-generation communications networks.

The current NATO strategy on emerging and disruptive technologies is to promote the development and adoption of dual-use technologies that will strengthen the Alliance's technological edge as well as help Allies protect themselves from adversaries, including terrorist groups, that may seek to use the emerging technologies of the Allies against them.

But the private sector is developing most emerging technologies. What will persuade industry to develop responsible business models that prioritize the well-being and safety of users and societies instead of profit? Additionally, can regulators keep up with the fast pace of scientific development to stop threat actors from exploiting gaps in the legislation or enforcement capabilities? Most legislative bodies take so long to pass and enact laws. By the time this process has been completed, the foundational models on which the laws have been based have likely advanced beyond recognition.

Thus, at the national and regional levels, governments have been trying to develop ethical frameworks with codes of conduct industry can adopt, thereby providing safeguards against and monitoring of known and emerging risks. Clearly, many visions are competing over how guardrails or safety regulations should be implemented effectively.

One approach has been for governments, leading technology organizations, academia, and civil society to come together to agree on ways to bake safeguards into specific technology areas. For example, following the first AI Safety Summit hosted by the United Kingdom in November 2023, the national cybersecurity agencies of 18 nations in the Americas, Europe, Asia, Australia, the Middle East, and Africa issued a set of "secure by design" guidelines to ensure countries and industries take security into account during the design, development, deployment, operation, and maintenance of an AI system.

Whether this approach will work remains to be seen. Nevertheless, NATO and member countries should consider supporting this process.

At a time of growing geopolitical competition, fewer resources are available for more traditional, collaborative counterterrorism efforts, like programs that build the capacity of local security forces or prevent and counter violent extremism. To fill some of the gaps, policymakers may fund proven technologies like surveillance drones and AI-powered applications. But shifting international power dynamics will make forging partnerships outside the Alliance for multilateral cooperation to counter emerging threats, including those arising from new technologies, more difficult.

A key tenet of NATO's policy guidelines is that countering terrorism remains primarily a national responsibility, while NATO's role is contributing to the global effort against terrorism in areas in which the organization can bring expertise and competence to the table. The collective strength of NATO comes into play here because no nation by itself can deal with the emerging threats malevolent actors pose through the weaponization of frontier technology.

Putting scientists and innovators in the same room as threat specialists and practitioners to forecast and devise threat scenarios and to help develop prevention and mitigation strategies and mechanisms is a good start.

— 1 —

Emerging Terrorist Threats: Everything, Everywhere, All at Once?

Susan Sim

Technology Trends That Will Shape Our Lives

In 2012, the World Economic Forum published its first list of the technology trends a panel of experts believed would have "the greatest impact on the state of the world in the near future."[1] As an exercise in "[shifting] the needle of global awareness" of the gap between new technological capabilities and their responsible development around the world, the World Economic Forum list was so widely read, it became an annual report on the top 10 emerging technologies.[2] Over the last decade, the list has identified "little-known technologies," such as the genetic-engineering tool, CRISPR-Cas9, featured in 2015, which is now being used to create insect- and drought-resistant crops, and messenger ribonucleic acid (mRNA) vaccines, first highlighted in 2017, which underpin the breakthrough COVID-19 vaccines now widely credited with protecting lives globally.[3]

The public's hunger for insight into new technologies has also spurred leading business magazines to put out their own annual lists. For instance, in November 2022, *Forbes* predicted that artificial intelligence (AI) would be everywhere in 2023, augmenting "nearly every job in every business process across industries"; part of the metaverse would become real with advances in augmented reality and virtual reality; blockchain technology would allow information to be stored and encrypted more innovatively and safely, allowing non-fungible tokens to become more usable and practical; digital-twin technology and 3D printing would bridge the digital and physical worlds; we would increasingly be able to "edit nature" by altering DNA, and nanotechnology would enable us to create materials with completely new features, such as water resistance and self-healing capabilities; and we would see even more self-driving trucks, ships, and delivery robots as a result of further progress in autonomous systems.[4]

Some emerging technologies—which the National Counterterrorism Center defines as innovative technologies that have been recently developed, are under development, or are likely to be developed in the next few years—are expected to offer solutions that will mitigate emerging crises in health care, food security, and climate change, whereas other emerging technologies are already changing lifestyles, improving work productivity, and enhancing the powers of the state. But multiple experts also believe new technologies like AI can cause fairly significant harm.[5] No one should thus be surprised some emerging technologies have lent, and will continue to lend, themselves readily to criminal or malevolent ends.

Technologies That Have Already Shaped the Terrorist Landscape

History is replete with examples of how new lethal and nonlethal technologies have driven fresh patterns of political violence, with the invention of dynamite in 1867 and the Avtomat Kalashnikova (AK-47) assault rifle in 1947 being the classic cases. That bombs and guns would become the terrorist's favorite weapons of mass destruction was not, however, something their inventors foresaw.

Alfred Nobel invented dynamite to solve the problem of gunpowder causing mining deaths in badly controlled explosions, which also created toxic gas clouds. The dynamite sticks Nobel patented and their explosive power when ignited by the blasting caps he also invented both made mining safer and accelerated the building of major infrastructure around the world, including the Panama Canal between 1904 and 1914. As "the first widely accessible, commoditized, inexpensive, and highly portable high explosive" that was safe and easy to use, dynamite also became the weapon of choice of anarchists, revolutionaries, and nationalists, spurring the first wave of modern terrorism, with bombings spreading to 52 countries between 1867 and 1934. Of the nearly 1,300 bombings reported during that period, most happened near dynamite factories.[6]

The second global surge of political violence was unleashed in the late 1950s when the Soviet Union began using the AK-47 assault rifle to spread Communism, selling the weapon cheaply to nonaligned countries and distributing free licenses to produce AK-47s in “fraternal countries.” Revolutionary when Mikhail Timofeyevich Kalashnikov first invented it as “the simplest automatic weapon possible” that could defeat the German firepower he experienced during World War II, the AK-47 quickly became “the world’s most prolific and effective combat weapon,” prized for its all-around ease of use and maintenance. Currently used by some 50 legitimate standing armies, the seemingly indestructible AK-47 is present in every conflict zone; is easy for insurgents, organized criminal groups, and terrorists to acquire; and is responsible for killing a quarter of a million people every year.[7]

Today, violent extremist groups also have a clutch of emerging technologies—autonomous vehicles, AI systems, 3D printing, augmented reality, and virtual reality—they can adapt to enhance the lethality of guns and bombs.

Take the increasingly ubiquitous unmanned aerial vehicles, more commonly known as drones. According to the 2023 *Global Terrorism Index*, some 65 non-state violent actors can now deploy drones because they are so “easily accessible in public marketplaces” and require little training to use.[8]

Drones have been around for more than a century; the British and US militaries developed the first pilotless, radio-controlled planes during World War I.[9] Although used during the Vietnam War to reconnoiter, launch missiles against fixed targets, and drop leaflets for psychological operations, drones did not enter the popular imagination until after the United States started using armed unmanned aerial vehicles to kill suspected militants following the September 11 attacks on the United States in 2001.

Terrorist groups, on the other hand, have been experimenting with drones to “diversify and bolster their capabilities” for about three decades. In 1993, the Japanese apocalyptic cult Aum Shinrikyo, in search of new ways to deliver sarin gas, tested a remote-controlled helicopter meant for crop spraying. Its plan was to assassinate a rival leader.[10] But even as it sought to perfect its bioweapon capabilities, Aum Shinrikyo never used a minicopter in its operations because the two that the group had apparently crashed during testing. Aum Shinrikyo thus launched its first public terror campaign in June 1994 with a refrigerator truck that the group equipped with a computer-controlled system to release a cloud of sarin into a residential neighborhood. Nine months later, on March 20, 1995, Aum Shinrikyo attacked the Tokyo subway, then the world's busiest underground transport system, with hand-delivered sarin packages, killing 12 and injuring 3,800 people.[11]

Drones have become much more sophisticated since the 1990s, with an array of military-grade, commercial, and hobbyist models available to non-state violent actors with different budgets, capabilities, and objectives. Since the Islamic State of Iraq and Syria began using jerry-rigged drones to drop small bombs or crash into coalition forces in Iraq and Syria in 2016, other violent actors have staged attacks as audacious as the 2018 assassination attempt on Venezuelan President Nicolás Maduro using commercial drones rigged with C-4, and as ambitious as the Yemeni Houthis disrupting a vital trade route by firing drones and missiles at commercial vessels sailing in the Red Sea during the Israel-Hamas War in Gaza. Even with a multinational force patrolling the waters, the threat has forced shipping lines to avoid the Red Sea and instead detour around Africa, driving up shipping costs and causing delivery delays.[12]

Drones are now on a trajectory to become fully autonomous weapons as a result of continuing efforts to integrate emerging technologies such as AI, robotics, nanoexplosives, and advanced computing into drones' systems so they can analyze data from sensors to identify objects and decide how to complete missions in "fire and forget" operations. Constant upgrades will make drones across the spectrum cheaper, smaller, able to fly longer, and able to carry heavier loads. Kai-Fu Lee, an AI researcher and entrepreneur, has that warned bird-sized drones will soon be able to fly themselves; seek out a particular person and shoot dynamite point blank through his or her skull; avoid being caught, stopped, or destroyed by being too small and nimble; and be built cheaply by hobbyists using parts bought online and open-source technologies. "And this is not a far-fetched danger for the future but a clear and present danger," Lee wrote in 2021 on the 20th anniversary of the September 11 attacks.[13]

How Threatening Are Emerging Technologies?

Is the diffusion of new technologies that offer mass destruction in the wrong hands turning terrorism into an everything, everywhere, all at once threat? In the past, only larger, resource-rich terrorist organizations could afford to innovate. But now, the increasing accessibility and affordability of modern technologies mean even small extremist cells and lone actors can carry out mass casualty attacks. To underscore "the complex and dynamic nature of the terrorist threat that we face today, which requires us to adapt and innovate constantly," the NATO Centre of Excellence Defence Against Terrorism (COE-DAT) chose "Searching for Trends in the Age of Turbulence: Everything, Everywhere, All at Once" as the theme of its flagship 2023 Terrorism Experts Conference in Ankara, Türkiye.[14]

Given the prevailing narrative that AI is on an inexorable march toward omnipotence, it is perhaps no accident that the conference theme references the award-winning Hollywood movie *Everything Everywhere All at Once*, a genre-bending, science fiction, action comedy playing on the idea of the multiverse and its "proliferating timelines and possibilities."[15] The movie's storyline is also an apt metaphor for how the line separating fiction from reality is blurring.

Indeed, UN Secretary-General António Guterres, in his *A New Agenda for Peace* policy brief, warned of the "perils of weaponizing new and emerging technologies" in terms that echo James Bond movie plots. "Advances in the life sciences have the potential to give individuals the power to cause death and disruption on a global scale," the UN secretary-general's July 2023 policy brief states, adding: "The emergence of powerful software tools that can spread and distort content instantly and massively heralds a qualitatively different, new reality."[16]

Is life imitating art? Replicating many of Hollywood's apocalyptic scenarios seems increasingly possible. In 2023, when the US Army War College Strategic Studies Institute, in partnership with the NATO COE-DAT, invited specialists on the front lines of terrorist-threat assessment and operational response to examine how emerging technologies might impact the terrorist landscape in the near term, the specialists came up with threat scenarios as terrifying as the UN secretary-general's. The specialists described how with access to tools such as nanotechnology, AI, automation, augmented reality, and other related technologies, terrorists might, in the next five years, be able to operate easily across borders; become stealthier and more lethal; and kill with tiny weapons, from the sky, or through the mass destruction of essential life supplies. (See chapters 2 through 6 of this publication for more in-depth discussions of these topics.)

But possibility is not feasibility. Why would terrorists use new technologies when existing weapons have worked so well? The most devastating and innovative terrorist attack of the last two decades involved four terrorists who went to flight school so they could fly commercial airplanes into symbols of American power like the twin towers of the World Trade Center and the Pentagon, killing 3,000 people in a single day.[17]

Even if we knew what advanced technologies terrorists are likely to exploit to further their goals of political intimidation and violence, is denying the terrorists access to the technologies feasible? If so, can we deny the terrorists access in a timely fashion?

The terrorist toolbox already contains sophisticated communications technologies like encrypted messaging apps and anonymization tools for secure and decentralized coordination among those planning attacks, their dispatchers, and operators. Many terrorist groups are also adept at using optimization tools on social media and online platforms to expand the groups' reach for recruitment and propaganda purposes. Some terrorist groups have also used augmented reality and virtual reality tools to conduct preattack activities, such as site reconnaissance and tactical information gathering, and may soon be able to stage face-to-face meetings with recruits without crossing borders. In other words, terrorist groups are using, and will continue to use, many publicly available technologies as they are designed to be used to enhance the groups' organizational capabilities and effectiveness.

In terms of terrorist tactics, the US intelligence community's current thinking is "most terrorist attacks during the next 20 years probably will continue to use weapons similar to those currently available—such as small arms and improvised explosives—because these are generally sufficient, accessible, and reliable."[18] But given most terrorist groups aspire to have "a lot of people watching and a lot of people dead," terrorist groups will also seize any opportunity to deploy novel weapons of mass destruction.[19]

In its *Global Trends 2040* report, the National Intelligence Council forecasts "technological advances, including AI, biotechnology, and the Internet of Things, may offer opportunities for terrorists to conduct high-profile attacks by developing new, more remote attack methods and to collaborate across borders." The report adds:

> Terrorists will also seek weapons of mass destruction and other weapons and approaches that will allow them to conduct spectacular mass casualty attacks. . . . Autonomous delivery vehicles guided with the help of AI systems could enable a single terrorist to strike dozens of targets in the same incident. Augmented reality environments could also enable virtual terrorist training camps, connecting experienced plotters protected by distant sanctuaries with potential operatives.[20]

For counterterrorism practitioners and policymakers, such long-term projections may be useful for resource planning, but as the 2023 *Annual Threat Assessment of the US Intelligence Community* notes, new technologies, especially in AI and biotechnology, "are being developed and are proliferating faster than companies and governments can shape norms, protect privacy, and prevent dangerous outcomes." The report also warns: "The convergence of emerging technologies is likely to create potentially breakthrough technologies not foreseeable by examining narrow science and technology areas, which could lead to the rapid development of asymmetric threats to US interests."[21]

In short, the risk of being blindsided is high if counterterrorism practitioners assume the past is prologue and fail to look for signs of terrorist organizations' technological aspirations and adaptation. Such demand-side analysis is usually based on available evidence that violent actors are motivated to invest in innovation for its impact—that is, evidence violent actors are interested in technology that is able to help them overcome security and logistical challenges and, importantly, will produce shock and awe when deployed, providing terrorists with a propaganda coup in a media-saturated environment.

Any technology-based threat assessment also must assess the supply-side issues: What obstacles might impede the process of non-state actors adopting and deploying technology, including financial and technical capacities? Crucially, what impediments might governments put in the way of violent actors procuring and deploying technologies?

But the history of drones suggests commercial and other pressures might make implementing preemptive measures to stop terrorists from exploiting emerging technologies very difficult for policymakers.

A Cautionary Tale of Drone (Mis)use

Military-grade drones were a restricted technology until local government agencies saw drones' potential for search-and-rescue missions and private companies wanted to use drones for labor-intensive tasks, such as inspecting pipelines, delivering goods to remote areas, and spraying pesticides on farms.[22] The exploitation of drones for commercial profit soon created a civilian drone industry wherein the United States alone currently contains some 727,000 commercial drones and 1.69 million recreational small drones, with the numbers forecast to continue growing.[23] The drone industry's growth has taken place in the last few years, as the Federal Aviation Administration, concerned more with air safety than terrorist ambitions, did not issue the first commercial drone permit until 2006, lifting some of the restrictions on flying consumer drones for recreational and business purposes.

Even then, the authorities were aware that , as Don Rassler has documented, four terrorist groups—the Japanese Aum Shinrikyo, the Colombia-based Revolutionary Armed Forces of Colombia, the Lashkar-e-Taiba, and the Haqqani network—were already exploring the use of unmanned aerial vehicles for terrorist attacks. The Lashkar-e-Taiba case involved a network of US residents who directly acquired sensitive technology from US companies in 2002 to enhance the performance of unmanned airplanes. Lashkar-e-Taiba intended to ship the technologies, which US companies could sell to domestic customers—mainly universities and the US government—without due diligence, for the group's military use in Kashmir. Several other terrorist groups also had their own drone programs, adapting Iranian models or reverse engineering stolen military drones—initially, for surveillance and the collection of tactical intelligence, external communications, and the smuggling of materiel into denied areas, and then, for use as weapons.[24]

Perhaps more interesting are the creative uses of drones individuals with no terrorist intent have found but that may cause harm, nonetheless. In December 2008, an American hobbyist successfully attached a pistol with a digital-camera gunsight to a minicopter and remotely fired the pistol. The hobbyist filmed his stunt and posted the footage online. The video did not attract much media attention, but almost seven years later, another American, a teenager, "upped the ante and the shock value" by mounting a homemade flamethrower to a small commercial drone he had modified and displaying the accuracy of the weapon in an online video.[25] Violent actors easily could have replicated both stunts to stage terrorist attacks.

Even after the hobbyists' stunts, several influential studies considered terrorists' use of drones a "niche threat" because few terrorist groups had successfully deployed drones in any meaningful way.[26] When the Islamic State of Iraq and Syria began weaponizing civilian drones and filming its attacks for propaganda purposes in 2016, several terrorism experts warned violent extremists could one day use drones as remote-controlled missiles to deliver unconventional weapons, such as deadly nerve agents.[27] Meanwhile, the general consensus remained that though drones might complicate conflicts, drones' broader impact would be limited, given their small payloads, short flight times, and susceptibility to disruption. Additionally, although technological advancements might make civilian drones more capable, "the tools to counter, disable or defeat [drones] will be more capable too," as will regulatory changes to restrict airspace access and increase export controls to prevent terrorists from acquiring certain technologies.[28]

Today, many governments require registrations for consumer drones that are heavier than seven kilograms. In addition, most governments have banned consumer drones from flying in cities, near sensitive installations, and over iconic events and other large gatherings, except with special permits. Since those with malevolent intentions usually do not apply for permits, jamming devices have also proliferated, as have geofencing technologies for disabling drones that are approaching designated no-fly zones.

Nonetheless, the Houthis' recent success in disrupting the Red Sea shipping route will likely inspire copycats. The Strait of Malacca, for instance, is another global trade route with several choke points. Any threat to shipping in this narrow channel bordered by Indonesia, Malaysia, Singapore, and Thailand will severely impact economies in East Asia and cause ripple effects throughout the rest of the world.

Weaponized drones will be a game changer for Southeast Asian terrorist groups. During the siege of Marawi City, Philippines, in June 2017, pro–Islamic State of Iraq and Syria militants reportedly used consumer-grade quadcopter drones to track, evade, and coordinate attacks on Philippine soldiers, inspiring the Philippine military to use similar drones.[29] But regional authorities apparently judged the drone use in Marawi City to be an outlier, a tactic imported by foreign fighters. The prevailing assessment is Southeast Asian terrorist groups like Jemaah Islamiyah and the various pro–Islamic State of Iraq and Syria offshoots in Indonesia and Malaysia will not expend their limited resources on drones when the supply of suicide bombers is seemingly unlimited. The use of drones for terrorist attacks is nevertheless a growing concern in Southeast Asia. Recent developments indicate Indonesian terrorists are hoping to acquire drone-warfare capability. In May 2023, the Indonesian counterterrorism unit Densus 88 obtained intelligence that Indonesian nationals whom the unit suspected of being affiliated with al-Qaeda in the Arabian Peninsula were undergoing training to fly drones in Yemen. Individuals affiliated with pro–Islamic State of Iraq and Syria militant factions were also sharing tutorials on how to make "drone bombs" with members of their private social-media chat groups.[30]

Challenge of Policing Emerging Technologies

Asking the Critical Questions

In its annual survey of the global risk landscape, the World Economic Forum has begun identifying risks associated with "the ever more rapid pace of technological development and its unprecedented intertwining with the critical functioning of societies." The forum's *Global Risks Report 2023* notes: "Technological risks are not solely limited to rogue actors. Sophisticated analysis of larger data sets will enable the misuse of personal information through legitimate legal mechanisms, weakening individual digital sovereignty and the right to privacy, even in well-regulated, democratic regimes."[31]

In contrast, the National Intelligence Council's *Global Trends 2040* report anticipates governments' surveillance capacities will expand to combat terrorists because of technological innovations, noting:

> Governments are likely to continue dramatically expanding the amount and types of information they collect as well as the tools to sort and organize that data. Advances in biometric identification, data mining, full-motion video analysis, and metadata analysis will provide governments with improved capabilities to identify terrorists and plotting. Development of precision long-range strike capabilities might undermine terrorist safe havens that are inaccessible to police or infantry forces.[32]

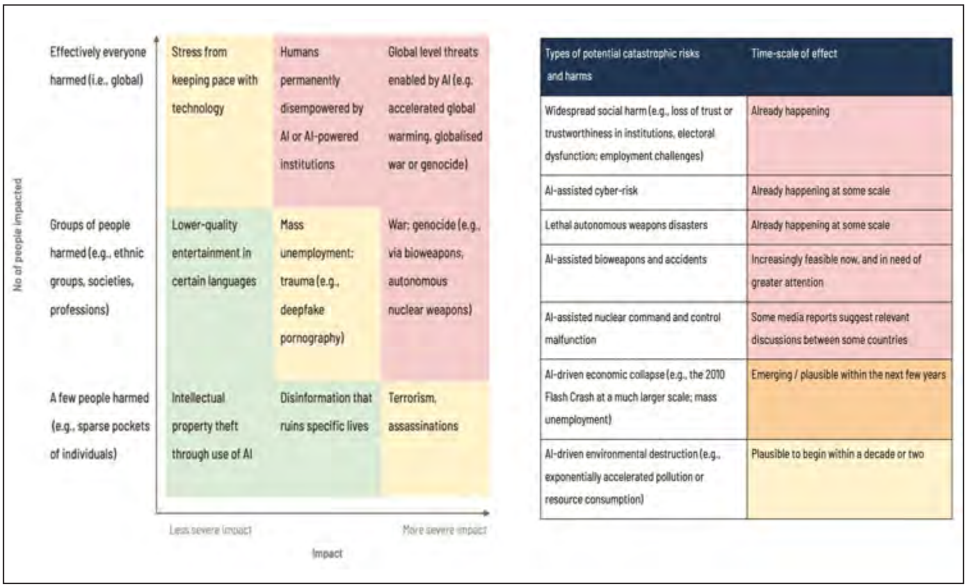
Apart from privacy concerns, which individual states must balance against security threats, some experts also caution against alarmism over the threat the potential misuse of AI and other emerging technologies poses of constructing "hypothetical dystopias where fact is indistinguishable from fiction."[33]

Clearly, countering terrorism must be part of a larger strategic consideration of the opportunities, risks, and harms of emerging and disruptive technologies. Often, an integrated approach requires asking the right set of questions.

With AI, for instance, many understand risks and harms might arise accidentally, intentionally, or due to stakeholders' willful indifference, and the impacts, levels of severity, and timescales of risks and harms will vary. Opinions on AI's risks and harms are diverse, and a key challenge is to "identify the critical questions of AI, that, if answered, will enable AI to truly be developed and deployed for the global good."[34] At the Singapore Conference on AI in December 2023, a group of about 40 global experts from academia, industry, and government worked to identify these critical questions. The group reached a consensus on some potential risks, the severity of their impact, and their estimated timescales.[35]

As figure 1-1 shows, the more severe impacts the group envisioned include acts of terrorism, the use of bioweapons targeting specific communities, and disasters involving autonomous weapons—harms that the group saw as already happening or increasingly feasible. The most catastrophic risks are mass extinction events, with experts seeing AI-driven environmental destruction as plausible in the next one to two decades.

Having identified the risks and harms considered catastrophic and thus deserving of greater attention, the group of experts advocated for the establishment of clear advance warning signs and thresholds across areas such as computing power; demonstrations of dangerous AI abilities; expert testimonies from diverse disciplines; and the proliferation of fake content, impersonations, and cyberattacks. By systematically defining indicators and possible responses ahead of time, governments can make decisions proactively and thus "avoid the 'boiling frog' by reacting only when problems become dire and harder to address." The group also recommended robust oversight mechanisms, including at the international level, for the most powerful AI systems, given their likely global impact.[36]



Effectively everyone harmed (i.e., global)	Stress from keeping pace with technology	Humans permanently disempowered by AI or AI-powered institutions	Global level threats enabled by AI (e.g. accelerated global warming, globalised war or genocide)
Groups of people harmed (e.g., ethnic groups, societies, professions)	Lower-quality entertainment in certain languages	Mass unemployment; trauma (e.g., deepfake pornography)	War; genocide (e.g., via bioweapons, autonomous nuclear weapons)
A few people harmed (e.g., sparse pockets of individuals)	Intellectual property theft through use of AI	Disinformation that ruins specific lives	Terrorism, assassinations

Types of potential catastrophic risks and harms	Time-scale of effect
Widespread social harm (e.g., loss of trust or trustworthiness in institutions, electoral dysfunction; employment challenges)	Already happening
AI-assisted cyber-risk	Already happening at some scale
Lethal autonomous weapons disasters	Already happening at some scale
AI-assisted bioweapons and accidents	Increasingly feasible now, and in need of greater attention
AI-assisted nuclear command and control malfunction	Some media reports suggest relevant discussions between some countries
AI-driven economic collapse (e.g., the 2010 Flash Crash at a much larger scale; mass unemployment)	Emerging / plausible within the next few years
AI-driven environmental destruction (e.g., exponentially accelerated pollution or resource consumption)	Plausible to begin within a decade or two

Figure 1-1. Potential risks of AI and estimates of the severity of the risks' impacts and timescales

(Source: *The SCAI Questions: Preliminary Conversations towards AI for the Global Good* ©Government of the Republic of Singapore, 2023)

Geopolitics of Regulating "Killer Robots"

A global race for technological dominance usually accompanies strategic competition between major powers, and when the world is in turbulence, as it currently is, weapons of great destructive power and ingenuity are often developed at a record pace. With AI weapons now projected to be the next revolution in warfare, Secretary-General Guterres has been pushing for greater regulation of the use of lethal autonomous weapon systems (LAWS). "The prospect of machines with the discretion and power to take human life is morally repugnant," Guterres told the UN General Assembly in September 2018.[37]

Despite widespread support for controls on the development of LAWS, which are defined as systems that use AI to select and attack targets without human intervention, current geopolitical tensions are impeding renewed attempts to set global rules. On December 22, 2023, with the support of 152 countries, the UN General Assembly adopted a resolution that stressed the urgent need to address challenges and concerns raised by LAWS, requiring the UN secretary-general to submit a substantive report with recommendations for discussion at the 2024 General Assembly. But 15 countries objected or abstained, including some of the leading developers of LAWS—namely, Russia, China, and Israel.[38]

Meanwhile, the race to develop “killer robots” continues, with proponents arguing autonomous weapons can be used responsibly to target only combatants. But will keeping “slaughterbots” out of the reach of non-state extremist actors be possible?

With LAWS looming on the horizon, the brief history of drones offers lessons on the difficulty of policing emerging technologies that are constantly progressing. The potential misuse of drones, which were developed as a military technology, was apparent from the beginning, as was drones’ great promise in “revolutionizing the business landscape.”[39] Drones are expected to be able to kill autonomously, enhance efficiency and safety across industries, and provide access to products and data from previously unreachable locations.

Regulating dual-use technologies (that is, technologies that have been developed primarily for commercial uses but may also be used for security and defense applications or malevolent purposes) has always been about balancing security with economic growth, with mitigation measures limited by available resources after rigorous risk assessments have been conducted. Absent an actual attack, government fiscal prudence requires clear evidence of a threat before policymakers will authorize investments in countermeasures.

With emerging technologies, governments face the dilemma of whether they should allow the development and likely proliferation of a new technology that might spur greater economic growth and impose regulations as threats emerge or try to control the technology’s development and risk stultifying scientific and economic progress. But the speed at which emerging technologies develop may not give governments much time to consider, weigh, and balance risks and opportunities and pass legislation. With much technological development now in the hands of private companies, governments may be playing catch-up most of the time, hoping that they can still shape norms and prevent dangerous outcomes and that private industry will not relentlessly prize profit above the safety and well-being of society.

A more proactive approach for which some governments have been advocating in recent years is shaping the ecosystem through strategic investments in the development and adoption of emerging technologies with dual uses. The North Atlantic Treaty Organization (NATO), recognizing technologies such as AI, autonomous systems, and quantum technologies are changing the way it operates, endorsed such a strategy in February 2021. Under *Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies*, NATO will work "with public and private sector partners, academia and civil society to develop and adopt new technologies, establish international principles of responsible use and maintain NATO's technological edge through innovation" as well as help Allies protect their technologies "from being used against them by potential adversaries and competitors."[40]

As part of the *NATO 2030*, agenda Alliance leaders also agreed to establish a multinational venture capital fund to support innovation in nine priority technology areas: AI, autonomy, quantum, biotechnologies and human enhancement, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, and next-generation communications networks.[41]

But one concern is that as nations increasingly view disruptive dual-use technologies as the critical frontier of strategic competition, nations may also start to view such emerging technologies as a zero-sum game. The first-ever *NATO Quantum Technologies Strategy*, approved in November 2023, outlines a vision for a quantum-ready NATO that emphasizes both the need for cooperation between Allies and the need for an investment climate that prevents, "on a voluntary basis," adversarial foreign investment in member countries' quantum ecosystems.[42]

The reality is that the "race between great powers to develop the most cutting edge and sophisticated approach to harnessing the promise" of emerging technologies like AI, autonomous systems, and quantum is ongoing.[43] Long before ChatGPT took the world by surprise and the term "large language model" entered the public lexicon, the United States and China were already investing billions of dollars in becoming the global leader in AI. Washington and Beijing continue to seek to leverage AI to complement and enhance their warfighting capabilities and combat-support activities as well as to support national security objectives, such as countering terrorism and engaging in domestic surveillance. Russia is far behind in terms of investments, but in 2017, President Vladimir Putin declared AI the future "for all humankind," adding: "It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."[44]

Some now consider Moscow a global leader in AI-driven asymmetric or hybrid warfare. Adapting Cold War–era "active measures"—that is, overt or covert operations aimed at influencing public opinion—to the digital age, Moscow has been using nonconventional tools hyperpowered by AI, such as cyberattacks, disinformation campaigns, and illicit finance, to project power and influence. Yet as several policy analysts have long concluded, "unlike in the conventional military space, the United States and Europe are ill-equipped to respond to AI-driven asymmetric warfare in the information space."[45] Change has been slow, even though the impact of asymmetric warfare waged on social-media platforms and elsewhere has become more obvious during elections, with the US government announcing symbolic criminal indictments of Russian troll farms in 2018 for election interference.[46]

Alongside hybrid warfare, Russia has also deployed non-state actors to foment domestic conflict abroad. Russia is not alone; just as the Soviet Union provided weapons like AK-47 rifles to local insurgent movements across the globe during the Cold War, Iran has been arming local militias in its neighborhood with weaponized drones and missiles to expand the country's sphere of influence.[47] Some groups—notably, the Houthis—have since been designated transnational terrorist organizations for their attacks on civilian targets outside the groups' original conflict zones.[48]

For any government, arming terrorist groups with advanced technologies like fully autonomous weapons to act as their non-state proxies would be an unpredictable bet, but such an occurrence is not outside the realm of possibility in a multipolar Cold War powered by emerging technologies.

Expanding the Counterterrorism Ecosystem

In the *NATO 2022 Strategic Concept*, NATO identifies terrorism as "the most direct asymmetric threat to the security of our citizens and to international peace and prosperity." Characterizing terrorist organizations as having "expanded their networks, enhanced their capabilities and invested in new technologies to improve their reach and lethality," the *Strategic Concept* goes on to state:

> Countering terrorism is essential to our collective defence. NATO's role in the fight against terrorism contributes to all three core tasks [deterrence and defence, crisis prevention and management, and cooperative security] and is integral to the Alliance's 360-degree approach to deterrence and defence. Terrorist organisations threaten the security of our populations, forces and territory. We will continue to counter, deter, defend and respond to threats and challenges posed by terrorist groups, based on a combination of prevention, protection and denial measures. We will enhance cooperation with the international community, including the United Nations and the European Union, to tackle the conditions conducive to the spread of terrorism.[49]

But as a NATO Defense College publication notes, the strategic concept mentions the issue of terrorism in various contexts, but terrorism "never receives coherent treatment," perhaps because "Allies diverge on their assessments of the terrorist threat as well as on the role that NATO should adopt in response."[50]

On the other hand, the Russian invasion of Ukraine in February 2022, which began while NATO was drafting the strategic concept, drove home the contours of the new strategic environment. The strategic concept states Russia is "the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area" because the country employs conventional, cyber, and hybrid means to undermine the rules-based international order in concert with the People's Republic of China. The strategic concept adds that China's "malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm Alliance security." Furthermore, the country "seeks to control key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains."[51]

Great-power competition has had two significant implications for counterterrorism: 1) it has displaced terrorism as the number-one national security threat in the United States, drawing away funds, personnel, and resources, including for international assistance, and 2) other alliances are increasingly challenging US leadership of global counterterrorism efforts.

The National Intelligence Council's *Global Trends 2040* report, for example, predicts: "Shifting international power dynamics—in particular, the rise of China and major power competition—

are likely to challenge US-led counterterrorism efforts and may make it increasingly difficult to forge bilateral partnerships or multilateral cooperation on traveler data collection and information-sharing efforts that are key to preventing terrorists from crossing borders and entering new conflict zones." Anticipating that decreases in counterterrorism assistance to other countries will continue, the report also notes that some "countries facing existential threats, such as insurgencies in which terrorists are active, may choose to forge non-aggression pacts that leave terrorists free to organize within their borders and others compelled to submit to terrorist rule over significant parts of their territory."[52]

Although fewer resources are available for the traditional capacity building of local security forces and programs for preventing and countering violent extremism, the United States and its allies could fill some gaps by judiciously funding proven technologies like surveillance drones and AI-powered applications.

At the same time, the prevention of terrorism in an age of powerful technologies must increasingly involve going further upstream and co-opting developers and designers of technology. Top cybersecurity officials in the West have been calling publicly for safeguards to be baked into AI. For instance, Jen Easterly, director of the Cybersecurity & Infrastructure Security Agency, warned in 2023 that without government guardrails, terrorists, cybercriminals, and adversarial nations could use AI capabilities for the "weaponization of cyber, a weaponization of genetic engineering, weaponization of biotech."[53]

Given that AI systems allow computers to recognize and contextualize data patterns without rules explicitly programmed by a human, making the systems vulnerable to adversarial machine learning, many governments are now trying to preempt the problems of the Internet era, in which technology and software developers have not always prioritized safety and security because doing so is not required. Rather, the developers have been leaving the problem of security flaws that allow malicious hacking and ransomware attacks to the multibillion-dollar cybersecurity industry to solve.

In November 2023, the United Kingdom hosted the first AI Safety Summit, which brought together governments, leading technology organizations, academia, and civil society from 28 countries in the EU and across the globe to address AI risks and to agree on "the need for inclusive and collaborative action."[54] The cybersecurity regulators of 18 nations in Africa, the Americas, Asia, Australia, Europe, and the Middle East have since come up with a set of Secure by Design guidelines, the purpose of which is to ensure security is taken into account during the design, development, deployment, operation, and maintenance of an AI system.[55]

Private-sector technology developers and operators will likely resist mandatory design rules, given the speed at which foundation models evolve and proliferate. For example, the obligatory reporting requirements proposed by the sweeping executive order on AI issued by the Biden-Harris administration in December 2023 for the developers of certain large models has been criticized as favoring incumbents that have greater resources to navigate the complex regulatory environment. At the same time, proponents of open-source AI models, including some of the models' founders, warn that the executive order's requirements to protect source codes may limit the public's ability to detect vulnerabilities in critical AI models, potentially allowing malicious actors to exploit the models. Others argue releasing detailed information about models may make exploiting vulnerabilities and reusing the models for unintended purposes easier for malicious actors.[56]

Clearly many competing visions exist for how guardrails or safety regulations can be implemented effectively. The United States and international partners' Secure by Design guidelines may succeed, given technology developers' involvement in forming the guidelines. To make guardrails effective, the next step would be to create a robust system of auditable safety and security standards and to award Secure by Design seals to products that meet these standards. Thus, even if not all nations agree to comply with the guidelines, technology developers may still be incentivized to follow the guidelines if government procurement offices, multinational corporations, and consumers at large are encouraged to purchase only the technology products bearing a Secure by Design seal.

The Secure by Design framework could also apply to other emerging technologies. Just as the big technology firms have somewhat belatedly come together in recent years, following pressure from several governments, to create advocacy groups like the Global Internet Forum to Counter Terrorism to mitigate the exploitation of their digital platforms by terrorists and violent extremists, so too the counterterrorism ecosystem should grow to encompass the developers and operators of emerging technologies, not just the regulators.

Growing the counterterrorism ecosystem would require greater awareness and understanding among counterterrorism practitioners and technology developers of their specialization's changing contours: How are terrorists innovating to exploit new technologies, and what else is coming down the technology pipeline that might interest malevolent actors? How might security practitioners leverage advanced technologies to predict and prevent terrorist attacks? For instance, online radicalization has lowered the barriers to entry to terrorism for young people who might now be able to 3D print a weapon or adapt off-the-shelf drones to stage a swarm attack. At the same time, even though governments now have more tools, it remains difficult for law enforcement agencies to detect lone actors who use readily available weapons and technologies unless they communicate their intentions to commit violence in advance.

The US military is using AI to support the processing, exploitation, and dissemination of critical information in conflict zones to enable commanders to increase their situational awareness and improve decision making. Counterterrorism practitioners have, to a lesser extent, also been relying on AI, primarily to aid the process of identifying and removing terrorism-related content from the Internet.[57] Privacy concerns have limited the use of AI in counterterrorism. Perhaps threat specialists can allay privacy concerns by sitting down with code writers to delineate the search parameters for seeking out domestic extremists that may be planning attacks.

Indeed, of the various strategies needed to deal with the emerging threats the weaponization of new technologies poses, the most important might be putting scientists, futurists, and innovators in the same room as counterterrorism specialists and practitioners so they can forecast threat scenarios and develop prevention and mitigation strategies and mechanisms.

Endnotes

1. Global Agenda Council on Emerging Technologies, "Top 10 Emerging Technologies for 2012," World Economic Forum (WEF) (website), February 15, 2012, https://www.weforum.org/agenda/2012/02/the-2012-top-10-emerging-technologies/.

2. Andrew Maynard, "One Hundred Emerging Technologies," *Andrew Maynard* (blog), December 9, 2021, https://andrewmaynard.net/2021/12/09/one-hundred-emerging-technologies/.

3. Centre for the Fourth Industrial Revolution, *Top 10 Emerging Technologies of 2023* (Cologny, CH: WEF, June 2023).

4. Bernard Marr, "The Top 10 Tech Trends in 2023 Everyone Must Be Ready for," *Forbes* (website), November 21, 2022, https://www.forbes.com/sites/bernardmarr/2022/11/21/the-top-10-tech-trends-in-2023-everyone-must-be-ready-for/?sh=227a222a7df0.

5. Janna Anderson and Lee Rainie, *As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035* (Washington, DC: Pew Research Center, June 2023).

6. Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (New York: Oxford University Press, 2020).

7. Larry Kahaner, "Weapon of Mass Destruction," *Washington Post* (website), November 25, 2006, https://www.washingtonpost.com/archive/opinions/2006/11/26/weapon-of-mass-destruction/72a246a2-4487-4162-b49d-8713f3bbb1c4/.

8. Institute for Economics & Peace (IEP), *Global Terrorism Index 2023: Measuring the Impact of Terrorism* (Sydney: IEP, March 2023).

9. "A Brief History of Drones," Imperial War Museums (website), n.d., accessed on November 10, 2023, https://www.iwm.org.uk/history/a-brief-history-of-drones.

10. Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology* (West Point, NY: Combating Terrorism Center at West Point, October 2016).

11. Kyle B. Olson, "Aum Shinrikyo: Once and Future Threat?," *Emerging Infectious Diseases* 5, no. 4 (July-August 1999): 513–16, https://doi.org/10.3201%2Feid0504.990409.

12. Willem Marx, "Houthis Launch More Drone Attacks as Shipping Companies Suspend Red Sea Operations," NPR (website), December 16, 2023, https://www.npr.org/2023/12/16/1219845584/houthis-red-sea-drone-attacks-ships-yemen-gaza; and Noam Raydan, "Rising Pressure on Red Sea Transit," Washington Institute for Near East Policy (website), December 22, 2023, https://www.washingtoninstitute.org/policy-analysis/rising-pressure-red-sea-transit.

13. Kai-Fu Lee, "The Third Revolution in Warfare," *Atlantic* (website), September 11, 2021, https://www.theatlantic.com/technology/archive/2021/09/i-weapons-are-third-revolution-warfare/620013/.

14. NATO Centre of Excellence Defence Against Terrorism (COE-DAT), *Terrorism Experts Conference Report* (Ankara, Türkiye: NATO COE-DAT, 2023).

15. A. O. Scott, "'Everything Everywhere All at Once' Review: It's Messy, and Glorious," *New York Times* (website), March 24, 2022, https://www.nytimes.com/2022/03/24/movies/everything-everywhere-all-at-once-review.html.

16. UN, *A New Agenda for Peace*, Our Common Agenda Policy Brief no. 9 (New York: UN, July 2023).

17. 9/11 Commission, *The 9/11 Commission Report* (New York: 9/11 Commission, 2004).

18. National Intelligence Council (NIC), *Global Trends 2040: A More Contested World* (Washington, DC: NIC, March 2021).

19. Brian Michael Jenkins, "The New Age of Terrorism," in *The McGraw-Hill Homeland Security Handbook*, ed. David G. Kamien (New York: McGraw Hill, 2006), 117–30.

20. NIC, *Global Trends 2040*.

21. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community* (Washington, DC: ODNI, February 6, 2023).

22. Amy Robinson, "FAA Authorizes Predators to Seek Survivors," Air Combat Command (website), July 27, 2006, https://www.acc.af.mil/News/Article-Display/Article/202994/faa-authorizes-predators-to-seek-survivors/.

23. Federal Aviation Administration, *FAA Aerospace Forecast Fiscal Years 2023–2043* (Washington, DC: Federal Aviation Administration, May 2023).

24. Rassler, *Remotely Piloted Innovation*.

25. Rassler, *Remotely Piloted Innovation*.

26. Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, MG-626-DTRA (Santa Monica, CA: RAND Corporation, 2008).

27. Joby Warrick, "Use of Weaponized Drones by ISIS Spurs Terrorism Fears," *Washington Post* (website), February 21, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

28. Rassler, *Remotely Piloted Innovation*.

29. Joseph Franco, "Preventing Other 'Marawis' in the Southern Philippines," *Asia & the Pacific Policy Studies* 5, no. 2 (May 2018): 362–69, https://doi.org/10.1002/app5.227.

30. Densus 88 officer, interview by the author, November 28, 2023.

31. WEF, *The Global Risks Report 2023*, 18th ed. (Cologny, CH: WEF, January 2023).

32. NIC, *Global Trends 2040*.

33. Peter Carlyon, "Deepfakes Aren't the Disinformation Threat They're Made Out to Be," *RAND Blog*, December 19, 2023, https://www.rand.org/pubs/commentary/2023/12/deepfakes-arent-the-disinformation-threat-theyre-made.html.

34. Government of the Republic of Singapore, "National Artificial Intelligence Strategy 2 to Uplift Singapore's Social and Economic Potential," press release, Smart Nation Singapore (website), December 4, 2023, https://www.smartnation.gov.sg/media-hub/press-releases/04122023/.

35. Government of the Republic of Singapore, *The SCAI Questions: Preliminary Conversations towards AI for the Global Good* (Singapore: Government of the Republic of Singapore, December 6, 2023).

36. Government of the Republic of Singapore, *SCAI Questions*.

37. António Guterres, "Address to the General Assembly" (speech, UN General Assembly Hall, New York, September 25, 2018), https://www.un.org/sg/en/content/sg/speeches/2018-09-25/address-73rd-general-assembly.

38. "UN General Assembly Adopts Resolution to Address 'AI Weapons,'" *NHK World-Japan* (website), December 24, 2023, https://www3.nhk.or.jp/nhkworld/en/news/20231224_14/ (page discontinued); and UN General Assembly, Resolution 78/241, Lethal Autonomous Weapons Systems, A/RES/78/241 (Dec. 28, 2023), https://documents.un.org/doc/undoc/gen/n23/431/11/pdf/n2343111.pdf?token=QvTTcCDxxHkCylEDHz&fe=true.

39. Marc Emmer, "Technology Trends for 2024 and Beyond," Vistage (website), October 30, 2023, https://www.vistage.com/research-center/business-financials/economic-trends/20231030-technology-trends-for-2024-and-beyond/.

40. "Emerging and Disruptive Technologies," NATO (website), June 22, 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm.

41. "Emerging and Disruptive Technologies."

42. "Summary of NATO's Quantum Technologies Strategy," NATO (website), January 17, 2024, https://www.nato.int/cps/en/natohq/official_texts_221777.htm.

43. "IntelBrief: Artificial Intelligence and Implications for International Security," Soufan Center (website), December 12, 2018, https://thesoufancenter.org/intelbrief-artificial-intelligence-and-implications-for-international-security/.

44. "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day," *Russia Today* (website), September 1, 2017, https://www.rt.com/news/401731-ai-rule-world-putin/.

45. Alina Polyakova, "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare," Brookings Institution (website), November 15, 2018, https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

46. Devlin Barrett, Sari Horwitz, and Rosalind S. Helderman, “Russian Troll Farm, 13 Suspects Indicted in 2016 Election Interference,” *Washington Post* (website), February 16, 2018, https://www.washingtonpost.com/world/national-security/russian-troll-farm-13-suspects-indicted-for-interference-in-us-election/2018/02/16/2504de5e-1342-11e8-9570-29c9830535e5_story.html.

47. Neil MacFarquhar, “The Proxy Forces Iran Has Assembled across the Middle East,” *New York Times* (website), October 27, 2023, https://www.nytimes.com/2023/10/27/world/middleeast/iran-proxy-militias.html?smid=nytcore-ios-share&referringSource=articleShare.

48. Anthony J. Blinken, “Terrorist Designation of the Houthis,” press release, January 17, 2024, https://www.state.gov/terrorist-designation-of-the-houthis/.

49. NATO, *NATO 2022 Strategic Concept* (Brussels: NATO, June 29, 2022).

50. Patrick Keller, “The New Status Quo Concept,” in *NATO’s New Strategic Concept*, ed. Thierry Tardy (Rome: NATO Defense College, 2022); and Thierry Tardy, “Six Takeaways from NATO’s New Strategic Concept,” in *NATO’s New Strategic Concept*, ed. Thierry Tardy (Rome: NATO Defense College, 2022).

51. NATO, *Strategic Concept*.

52. NIC, *Global Trends 2040*.

53. John Curran, “Easterly Voices Urgent Need to Set AI Regulatory Landscape,” MeriTalk (website), April 7, 2023, https://www.meritalk.com/articles/easterly-voices-urgent-need-to-set-ai-regulatory-landscape/.

54. “The Bletchley Declaration by Countries Attending the AI Safety Summit,” United Kingdom Government (website), November 1, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023; and Claire W., “Introducing the Guidelines for Secure AI,” *National Cyber Security Centre* (blog), November 27, 2023, https://www.ncsc.gov.uk/blog-post/introducing-guidelines-secure-ai-system-development.

55. Claire W., “Guidelines for Secure AI.”

56. “IntelBrief: Tensions between Transparency & Security in Biden’s Executive Order on Artificial Intelligence,” Soufan Center (website), December 15, 2023, https://thesoufancenter.org/intelbrief-2023-december-15/.

57. “Artificial Intelligence and Implications.”

— 2 —

ChatGPT, Artificial Intelligence, and the Terrorist Toolbox

Sarah Lohmann, PhD

Introduction

In 2021, the UN Counter-Terrorism Centre and the UN Interregional Crime and Justice Institute warned, "As soon as AI becomes more widespread, the barriers to entry will be lowered by reducing the skills and technical expertise needed to employ it. . . . AI will become an instrument in the toolbox of terrorism."[1]

This time has now come. The massive global use of Chat Generative Pretrained Transformer, popularly known as ChatGPT; of drones; and of biometrics as everyday artificial intelligence (AI) tools has hastened the lowering of barriers to entry due to the misuse of the tools and a lack of regulation, rather than the innovators' intent. The NATO AI strategy calls for ensuring AI is deployed lawfully and used in a way that promotes traceability, reliability, and governability.[2] At the same time, NATO has committed to new capabilities and technologies, including in the area of AI, to counter terrorism and terrorist use of such technologies.[3]

This study analyzes how terrorists are using AI to expand their power and reach and training followers to do so for the foreseeable future. Specifically, the chapter outlines the AI toolbox terrorists are using for hacking weapons systems; for violence with drones and self-driving car bombs; and applying bots for outreach, recruitment, and planning attacks.

TOC

After a discussion of the technical tools terrorists are using and their impact, the chapter discusses the current AI regulatory framework in Latin American countries as compared with new governance initiatives in the EU. The chapter concludes with mitigation and governance recommendations for NATO's counterterrorism purposes.

ChatGPT as a Terrorist Recruitment Tool?

On November 30, 2022, OpenAI made ChatGPT publicly available for free to allow users to generate content based on prompt engineering—a series of prompts and replies that uses an AI chatbot based on a large language model.[4] The content ChatGPT produces has been taken from the Internet, but the AI has been trained on language written by humans, so the text the AI produces is often startling in its ability to copy human composition and casual speech. No wonder by January 2024, ChatGPT had become the fastest-growing consumer software application in history, with more than 100 million users.[5] Already in December 2023, a Daesh user posted on Rocket.chat that he had used the free ChatGPT AI software tool for advice on how to support the caliphate. The user reported ChatGPT had supplied him with instructions on how to rally a core group of supporters and how to develop a political program and ideology. ChatGPT, which saw several upgrades in 2023 and limitations set by the system's programmers on the type of information it can answer, refused to respond to questions on how to build a bomb or join a rebel religious group.[6]

In fact, as part of the model's content moderation policy, ChatGPT has been programmed not to answer questions that contain harmful or biased content. Although the tool is constantly being updated to filter more effectively and not to repeat such content, occasionally, the correct prompt engineering overrides such filters.[7]

ChatGPT has been used to improve phishing emails, plant malware in open-coding libraries, spread disinformation, and create online propaganda.[8] Areas where ChatGPT is still learning what qualifies as harmful could include online terrorism training or how to create firearms or lethal components needed for an attack.[9] The tool and other AI platforms, which include AI-driven chatbots, could be used to develop dialogue to build trust and gain information or to impersonate an identity to compromise national security.[10]

Now, international organizations are looking into how to regulate the technology. Although the creators of ChatGPT have come up with a set of initial, self-imposed regulations, other AI platforms have fewer controls.

The AI platform Perplexity Ask, which did not have the same technical limitations, provided detailed directions on how to behead someone or make ricin. Neo-Nazi and other violent extremist organizations have used both AI platforms.[11]

Cybercriminals and terrorists have quickly become adept at using such platforms and large language models in general to create deepfakes or chatbots hosted on the dark web to obtain sensitive personal and financial information or to plan terror attacks or recruit followers. This malicious use is likely to increase in the future as the models become more sophisticated. How sensitive conversations and Internet searches are stored and distributed over AI platforms or via large language models will require more transparency and controls.[12]

Terrorist Use of AI with Big-Data Analytics

Terrorists are also using AI paired with big-data analytics to hack secure systems. Why? The terrorists do not have to put their lives at risk with direct personal contact with their victims, nor do the terrorists need great amounts of funding. The terrorists can sit behind a computer and use social media to access biometrics.

Artificial intelligence provides facial, fingerprint, iris, and behavior recognition, but digital biometrics can be stolen. Biometric identification methods can be hacked by stealing biometrics from an online source or even using biometrics from a recently deceased person. Machine learning has progressed to the point that it can teach the AI in biometric systems to recognize the difference between living and dead irises—with one exception. The system was able to tell the difference between living and dead irises in databases with 99-percent accuracy. The challenge was the person had to be deceased for at least 16 hours to be counted as dead.[13]

Trend Micro's 2022 report on the malicious use of biometrics by cybercriminals—including through the exposure of faces, retinas, irises, ear-shape patterns, and in some cases, palms and fingerprints—shows just how easy using biometrics over social media has become.[14] Social media sites like TikTok and Instagram have millions of images and videos with close-up images of eyes, such as videos that show the application of makeup, or ears, such as images that advertise earrings. Twitter exposed high-resolution images of thumbprints, while even seemingly harmless communication platforms like Viber, Telegram, and WhatsApp and social media platform Facebook provide voice patterns and palm shapes that could easily be extracted and, in some cases, geolocated and time-stamped.[15]

Because biometrics are used for access to places of high national security value, such as chemical, biological, radiological, and nuclear research labs, banks, or stock market access, exfiltrating these sensitive characteristics could enable malicious actors to cause drastic damage. For instance, terrorists could use hacked biometrics to release pathogens from a lab, force a stock market crash, or spy on civilians using tracking tools. Also of great concern is the amount of government officials' biometric data available, even on government websites. For example, on the website of the European Commission, users can find portraits of government officials with over 10 megapixels of resolution.[16] The site, which is easily searchable, allows the free use of 50,000 photos and 120,000 videos of government officials; audio files are also available.[17] Biometric eye and fingerprint data and voice patterns are easily extracted from these high-quality files.[18]

Malicious actors have used high-resolution photographs to create dummy eyes or three-dimensional-printing faces to bypass biometric tests, according to Keiron Shepherd, security solution architect for Northern and Western Europe at the cybersecurity firm F5.[19] Biometric data can also be used to create deepfakes. Biometric data cannot be reset as passwords can, and risks to general users are likely to improve as device cameras improve. The good news is biometric systems today implement security that involves algorithms and sensors that can differentiate whether a physical trait is from a living individual or has been hacked.[20] To protect against fraudulent or terroristic use of biometrics, multifactor authentication provides a formidable defense. Multifactor authentication includes public key infrastructure–based (PKI-based) digital certificates, rather than just biometrics, for verification.[21] Making employees—especially those in the national security, financial, or defense research and development sectors—and their families aware of the dangers of uploading biometric information should be part of every onboarding process in these sectors as well.

TOC

Using Unmanned Aerial and Self-Driving Vehicles to Kill

Two Global Positioning System–guided drones carrying explosives targeted Venezuelan President Nicolás Maduro in an August 2018 assassination attempt.[22] But Venezuela is not the only place unmanned aerial vehicles (UAVs) are being used to kill. The Houthis have targeted oil facilities and other critical infrastructure in Saudi Arabia; Daesh has used commercial UAVs in Iraq and Syria; and the UN recorded the first completely autonomous, AI-based drone strike in Libya in 2020. According to a Cambridge University Press study that used the Global Terrorism Database, 76 terror attacks between 2016–19 involved UAVs, 47 of which were successful and resulted in 50 deaths and 132 injuries.[23] In the years since, drones have increasingly been used on the battlefield, and improved AI has enabled ever-greater precision, even among commercially available UAVs, making them cheap tools of choice for terrorists.

Terrorists have experimented with the possibility of using drones and self-driving car bombs to execute attacks for years.[24] Christopher Wray, the director of the FBI, warned about the danger of self-driving vehicles being targeted and used as a weapon by malicious actors in 2023 at the World Economic Forum.[25] Indeed, terrorists can already hack traffic-guidance systems to create deadly attacks.[26]

Although terrorists have used rental trucks to carry bombs or drive into a group of people for decades, fully autonomous, self-driving vehicles are still in the testing phase in most places. As of December 2022, 38 states in the United States allowed autonomous vehicles to be tested on public roads, with Arizona, California, Michigan, New Hampshire, and Ohio, allowing them to be on public roads completely driverless.[27] The Insurance Institute for Highway Safety expects 3.5 million self-driving vehicles to be on US roads by 2025.[28] In Latin America, Brazil leads the market in the adoption of self-driving cars. Brazil has the most automated vehicles on the road due to its infrastructure being interconnected.[29] Latin America has a projected compound annual growth rate from 2022–24 of 28.5 percent and $3.75 billion.[30] Nevertheless, currently, Brazil has no laws to regulate the use of autonomous vehicles.[31] With the autonomous-vehicle market growing in both North America and Latin America and self-driving cars becoming as easily available to potential terrorists as rental trucks, a new regulatory framework will be needed as soon as possible.

TOC

In any framework, external control of driverless vehicles should be considered. Although driverless vehicles have been built to follow the directions of their human owners, driverless vehicles can also receive their instructions from a traffic-guidance system. Such a system could be used to help to prevent a crash, facilitate a nonviolent law-enforcement stop, or ensure emergency service vehicles pass more quickly. However, with traffic-guidance systems being connected through the Internet of Things and terrorists hacking systems to target victims or to perpetrate terror attacks, emergency control systems must urgently be adapted to provide passengers with an override option so civilian life can be protected. In addition, driverless cars could be used for trafficking drugs and other contraband. Both trafficking and the manipulation of destination and routing can be prevented by installing multiple sensors to compare inputs and send warnings that sensors or software have been manipulated or altered.[32]

In the case of traffic systems being hacked, researchers working for the Swedish Transport Administration and the KTH Royal Institute of Technology have recommended installing automatic communication systems that warn other vehicles in the vicinity as well as equipping cars with facial or biometric identification mechanisms.[33] Because biometrics can also be faked and customers can be kidnapped to enable software alterations at a terrorist's directive, installing new identification systems will be necessary.

Creating a New AI Regulatory Framework for the Americas

Clearly, although the broader public will continue to use AI to secure and improve the way people use lifesaving data, terrorists will continue to use the same AI tools for recruitment, hacking, and physical destruction. So how can North and Latin American governments create a regulatory framework that limits terrorists' access to AI tools and their potentially destructive impact? The current policy dialogue focuses more on impact and controlling the technology, rather than access or punishing malicious users. In the United States, the Federal Trade Commission has been investigating OpenAI because the data ChatGPT supplies in response to queries can be pulled from anywhere on the web, including propaganda or disinformation sources, creating the potential for the distribution of false data or the compromising of personal or professional reputations.[34]

In October 2022, the White House published the *Blueprint for an AI Bill of Rights*. Among other measures, the White House calls for AI systems to be tested and monitored before deployment, and for an intervention to occur if they are not used safely.[35] Although such a blueprint is not binding, Congress is working on draft legislation to curb use that would endanger national security. Senators Richard Blumenthal (Democrat, Connecticut) and Josh Hawley (Republican, Missouri) have proposed a bipartisan framework that would establish an independent oversight body to regulate the use of AI in facial-recognition technology and ChatGPT-4, curb the harmful use of deepfakes, and levy export controls or sanctions when advanced AI models are transferred to China, Russia, or "countries engaged in gross human rights violations."[36] In this framework, AI developers can be held liable if their products caused harm.

Although North America has no comprehensive regional law on AI, the EU, the African Union, the Group of Seven, and the Group of 20 have developed regional approaches to AI. In addition, 60 countries have national AI strategies. In 2019, the Organisation for Economic Cooperation and Development adopted its AI Principles—the first intergovernmental organization to do so.[37] Currently, the EU's Artificial Intelligence Act, which categorizes AI-enabled technologies according to the risk they pose to health, safety, and human rights, may be the most comprehensive.[38] The law, passed in March 2024, curbs real-time facial recognition and creates new transparency requirements for AI tools like ChatGPT.[39] This law could serve as a model for the Americas.

So far, none of the legislative proposals have directly addressed the urgent question of misuse of the technology by terrorists. Much like the early legislation passed in the last decade to regulate social media, platform innovators, developers, and owners are held to account, but not those who would use positive innovation for nefarious purposes. Latin America is no exception.

Working closely with the Organisation for Economic Cooperation and Development, the Latin American and Caribbean (LAC) countries are creating an ethical and human-centric approach to AI. Seven LAC countries have adopted, or are in the process of adopting, their own national AI strategy: Argentina, Brazil, Chile, Colombia, Mexico, Peru, and Uruguay.[40] Although individual countries have made progress on AI ethics, governance, and adoption as well as cross-sector collaboration and procurement and policies on data and technical infrastructure, the LAC countries have not formulated a regional strategy.[41] Table 2-1 illustrates the implementation progress of the AI plans for six of the previously mentioned countries, as rated by the Organisation for Economic Cooperation and Development.[42]

Table 2-1. Implementation progress of AI plans in LAC countries

Country	Objectives and Specific Actions	Measurable Goals	Responsible Actors	Time Frames	Funding Mechanisms	Monitoring Instrument
Argentina	√	√	√	Partially	X	X
Brazil	√	X	X	X	X	X
Chile	√	√	√	Partially	X	X
Colombia	√	√	√	√	√	√
Peru	√	X	X	X	X	X
Uruguay	√	Partially	X	X	X	

Users of ChatGPT in countries such as Brazil are already concerned the new AI tool is violating the rules LAC countries have in place, such as the Brazilian General Data Protection Law. Brazil's law, much like Europe's privacy laws, requires the origin of data be clearly labeled and that any personal data used, such as data entered into a website or used to train a language model, be made clear and accessible to users.[43] Although several LAC countries have similar data protection laws, the AI strategies referenced in figure 2-1 do not yet have up-to-date policies on how to limit access to or misuse of AI tools such as ChatGPT or AI-recognition tools.[44]

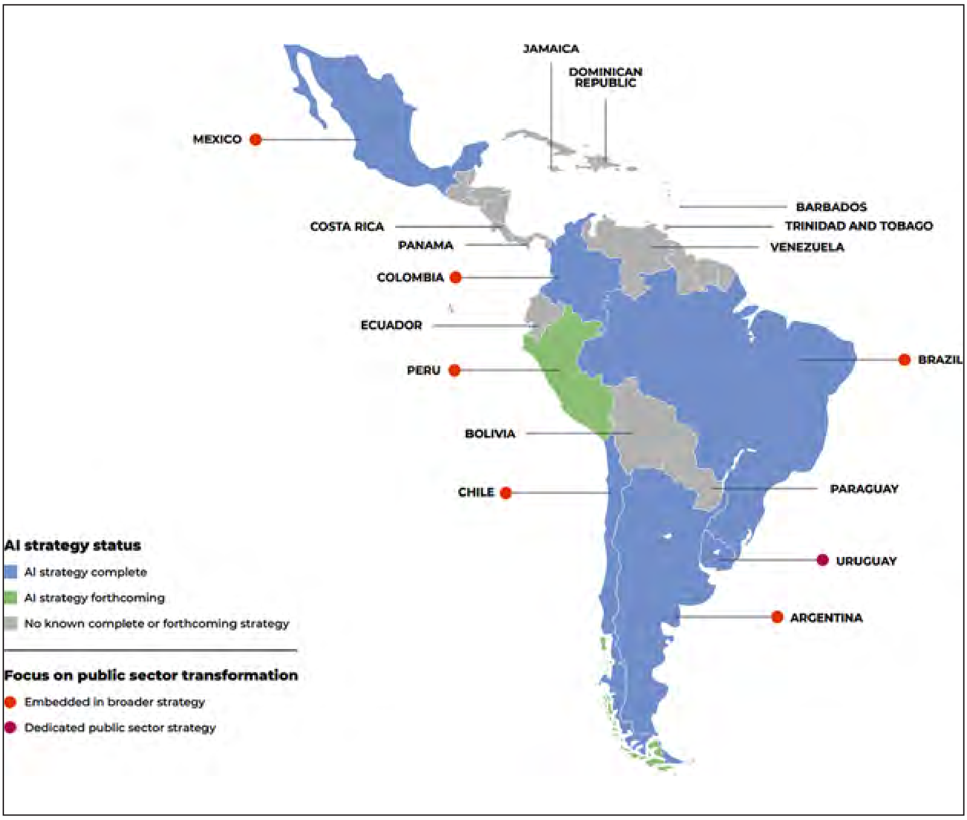


Figure 2-1. The LAC countries' AI strategy statuses

Why does this lack of up-to-date policies matter when the tool is open and free for use by terrorists? Prompts for the tool, such as where a certain person lives (that is, the target) or how to carry out an attack (that is, the methodology), receive responses that mix all sources from the Internet together, including true and false information. In a recent call with journalists, the FBI outlined its concern that ChatGPT has already been consulted by terrorists for information on how to launch chemical attacks or alter chatbots' application programming interface, allowing it to generate malware.[45]

Without additional regulation, which should include sourcing and filters to separate fact from fiction as well as strong malware guards, the tool could continue to be misused.

Conclusion

Terrorists have shown themselves to be adept at using new AI technology, from ChatGPT to drones and from biometrics to self-driven cars. Although current legislative efforts in the Americas focus on regulations and liability for AI companies, an additional framework is needed to address terrorist and cybercriminal use of the technologies. This framework must include both technological protections and judicial and regulatory mechanisms to ensure malicious use is prevented. As NATO seeks to fulfill its mandate to counter terrorism and terroristic use of emerging and destructive technology, the organization should continue to promote traceability, reliability, and governability as NATO seeks to protect civilian populations who may use or be impacted by the terroristic use of drones, biometrics, and self-driven cars.

The Alliance can achieve these objectives by encouraging good governance in addressing the storage and distribution of sensitive conversations and Internet searches on AI platforms and AI companies' labeling of false or damaging information on ChatGPT prompts. Using PKI–based digital certificates to protect biometrics and human-resources education campaigns for high-target employees and their families is more necessary now than ever before. Counter-UAV capabilities and policies for protecting civilian life will remain a critical NATO capability as commercial drones are increasingly used by non-state actors and terrorists.

As the driverless-car market grows drastically in the Americas, passenger override options, duplicative sensors, hardened traffic-guidance systems, and car-to-car communication systems will be necessary to ensure the protection of human life. Just as pertinent will be judicial and legislative frameworks that ensure terrorists and cyber hackers are held to account for the malicious use of the technologies. Regulations should ensure that access to self-driving cars for malicious purposes becomes as limited as possible through new user-identification methods. For these technology and policy mechanisms to succeed, policymakers, industry, and the NATO community will need to work together to ensure AI innovation continues to improve member states' security, not challenge it.

Endnotes

1. UN Counter-Terrorism Centre (UNCCT) and UN Interregional Crime and Justice Research Institute (UNICRI), *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes* (New York and Turin, IT: UNCCT and UNICRI, 2021), 7.

2. NATO, *NATO's Data and Artificial Intelligence Review Board* (Brussels: NATO, October 13, 2022).

3. "Countering Terrorism," NATO (website), July 19, 2023, https://www.nato.int/cps/en/natohq/topics_77646.htm.

4. "What Is ChatGPT?," OpenAI (website), n.d., https://help.openai.com/en/articles/6783457-what-is-chatgpt.

5. Krystal Hu, "ChatGPT Sets Record for Fastest-Growing User Base – Analyst Note," Reuters (website), February 2, 2023, www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

6. Steven Stalinsky, "Terrorists Love New Technologies. What Will They Do With AI? | Opinion," *Newsweek* (website), March 14, 2023, https://www.newsweek.com/terrorists-love-new-technologies-what-will-they-do-ai-opinion-1787482.

7. Europol Innovation Lab, *ChatGPT: The Impact of Large Language Models on Law Enforcement* (The Hague: EU Agency for Law Enforcement Cooperation, March 2023), 4.

8. Europol Innovation Lab (EIL), *ChatGPT*, 8–10.

9. Yaser Esmailzadeh, "Potential Risks of ChatGPT: Implications for Counterterrorism and International Security," *International Journal of Multicultural and Multireligious Understanding* 10, no. 4 (April 2023): 535–43.

10. Esmailzadeh, "Potential Risks of ChatGPT," 535–43.

11. Stalinsky, "Terrorists Love."

12. EIL, *ChatGPT*, 11.

13. Deniz Yurdasen, "How Artificial Intelligence (AI) Is Used in Biometrics," Aratek (website), April 20, 2023, www.aratek.co/news/how-artificial-intelligence-ai-is-used-in-biometrics.

14. Craig Gibson et al., *Leaked Today, Exploited for Life: How Social Media Biometric Patterns Affect Your Future* (Tokyo: Trend Micro, 2022).

15. Gibson et al., *Leaked Today*, 7–8.

16. "Search Results (56210)," European Commission (website), n.d., accessed on September 18, 2023, https://audiovisual.ec.europa.eu/en/search?mediatype=PHOTO&categories=Portrait.

17. Gibson et al., *Leaked Today*, 12.

18. Gibson et al., *Leaked Today*, 12.

19. Giulia Carbonaro, "Can Videos Uploaded on Social Media Allow Hackers to Steal Your Biometric Data?," *Euronews* (website), October 27, 2022, https://www.euronews.com/next/2022/10/27/can-videos-uploaded-on-social-media-allow-hackers-to-steal-your-biometric-data.

20. Carbonaro, "Your Biometric Data."

21. Carbonaro, "Your Biometric Data."

22. Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, Land Warfare Paper no. 137 (Arlington, VA: Association of the US Army, February 2021).

23. Dennis Barten et al., "A Counter-Terrorism Medicine Analysis of Drone Attacks," *Prehospital and Disaster Medicine* 37, no. 2 (2022): 192–96, https://doi.org/10.1017/S1049023X22000139.

24. Stalinsky, "Terrorists Love."

25. Johnna Crider, "FBI Director Says Self-Driving Cars Could Era in New Terror Attack Opportunities," Teslarati (website), January 19, 2023, https://www.teslarati.com/fbi-director-self-driving-terrorism/.

[26] Sven Ove Hansson, Matts-Åke Belin, and Björn Lundgren, "Self-Driving Vehicles—An Ethical Overview," *Philosophy and Technology* 34 (August 12, 2021): 1383–408, https://doi.org/10.1007/s13347-021-00464-5.

[27] "Autonomous Vehicles," Governors Highway Safety Association (website), n.d., accessed on December 21, 2023, www.ghsa.org/issues/autonomous-vehicles; and "Autonomous Vehicle State Bill Tracking Database," National Conference of State Legislatures (website), July 20, 2022, www.ncsl.org/transportation/autonomous-vehicles-state-bill-tracking-database.

[28] "Autonomous Vehicles," National Association of Insurance Commissioners (website), December 20, 2022, https://content.naic.org/cipr-topics/autonomous-vehicles.

[29] Kenneth Research, *Latin America Self-Driving Car Market (2018–2024)* (New York: Kenneth Research, October 2022).

[30] James Smith, "Latin America Self-Driving Car Market Investment, Growth Forecasting and Insights through 2032," *Taiwan News* (website), November 7, 2023, https://www.taiwannews.com.tw/en/news/5035199.

[31] Pedro Goncalves, "Autonomous Cars: Challenges and Perspectives," Institute for Research on Internet and Society (website), April 15, 2017, https://irisbh.com.br/en/autonomous-cars-challenges-and-perspectives/.

[32] Hansson, Belin, and Lundgren, "Self-Driving Vehicles," 34.

[33] Hansson, Belin, and Lundgren, "Self-Driving Vehicles," 34.

[34] "What Are Governments Doing to Try to Regulate AI?," Reuters (website), September 11, 2023, https://www.euronews.com/next/2023/09/11/which-countries-are-trying-to-regulate-artificial-intelligence.

[35] Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Washington, DC: White House, October 2022).

[36] Richard Blumenthal and Josh Hawley, *Bipartisan Framework for US AI Act* (Washington, DC: Senate Subcommittee on Privacy, Technology, and the Law, September 2023).

[37] Organisation for Economic Cooperation and Development (OECD) and Corporación Andina de Fomento (CAF), *The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean* (Paris and Caracas: OECD and CAF, 2022).

[38] Patricia Scanlon, "OPINION: America Should Learn from Europe and Adopt Tougher Regulations on Artificial Intelligence," Hechinger Report (website), September 18, 2023, https://hechingerreport.org/opinion-america-should-learn-from-europe-and-adopt-tougher-regulations-on-artificial-intelligence.

[39] Billy Perrigo and Anna Gordon, "E.U. Takes a Step Closer to Passing the World's Most Comprehensive AI Regulation," *TIME* (website), June 14, 2023, https://time.com/6287136/eu-ai-regulation/.

[40] OECD and CAF, *Strategic and Responsible Use*.

[41] OECD and CAF, *Strategic and Responsible Use*.

[42] OECD and CAF, *Strategic and Responsible Use*.

[43] Luca Belli, "Why ChatGPT Does Not Comply with the Brazilian Data Protection Law and Why I Petitioned the Regulator," *Medianama* (website), May 25, 2023, https://www.medianama.com/2023/05/223-chatgpt-brazilian-data-protection-law-ai-regulation/.

[44] OECD and CAF, *Strategic and Responsible Use*.

[45] Alex Blake, "Hackers Are Using AI to Create Vicious Malware, Says FBI," *Digital Trends* (website), July 31, 2023, https://www.digitaltrends.com/computing/hackers-using-ai-chatgpt-to-create-malware/.

— 3 —

Weaponizing Food Insecurity: The Violent Extremist Threat to Precision Agriculture in the United States

Michael W. Parrott

Introduction

The agriculture industry has predominately been a mechanical and manual labor trade for centuries. With recent advancements in the technology sector, autonomous devices, sensors, and information systems are saturating the agriculture industry at an unprecedented rate. Economic investment futures forecast a significant growth in unmanned systems within the agriculture and logistics industries over the next five to 10 years.[1] This growth is driven by drones and data applications, which are used to replace mechanical processes with more precise technological methods. The proliferation of unmanned systems throughout the agriculture and logistics sectors increases the probability that threat actors, such as violent extremists, will exploit and weaponize commercial drones, which lack the more stringent security protocols found within the defense industry.

The threat from these substate terrorists to domestic and international food-supply depots and production facilities poses a direct threat to America's homeland and national security. Substate terrorism denotes terrorism within five subcategories: leftist social revolutionary terrorism, right-wing terrorism, nationalist-separatist terrorism, single-issue terrorism, and religious extremist terrorism. Religious extremist terrorism is broken down further into new-religions terrorism and religious fundamentalist terrorism; al-Qaeda and the Islamic State in Iraq and Syria fall into the latter subcategory.[2] Violent extremist organizations (VEOs) like al-Qaeda and the Islamic State in Iraq and Syria have successfully employed drone attacks in Africa, Asia, the Americas, Europe, and the Middle East increasing the probability of drone attacks in the future. In 2002, as US and coalition forces gained control of al-Qaeda territory in eastern Afghanistan, they uncovered a treasure trove of documents. "Among the thousands of documents they discovered were US agricultural documents and al Qaeda training manuals targeting agriculture," according to Dean Olson.[3] Al-Qaeda and the Islamic State in Iraq and Syria's homegrown terrorist sympathizers have successfully carried out attacks in the United States, adding a layer of complexity to an already perilous threat. This chapter postulates within the next decade, religiously motivated terrorists (RMTs) like al-Qaeda, the Islamic State in Iraq and Syria, and their affiliates and adherents could leverage technological advancements in unmanned systems within the agriculture sector to conduct catastrophic attacks on the American agriculture industry and cause further global food insecurity and economic costs.

Research Methodology and Scope

This chapter uses a case-study approach to examine the likelihood of RMTs using unmanned systems to conduct attacks on the American agriculture industry (and thereby causing economic fallout) in the not-so-distant future. Current literature describes the agriculture industry's increasing reliance on drones and associated technology as well as the vulnerabilities this new technology creates and provides examples of how terrorists might exploit the technology to threaten the agriculture sector. The vignettes in this paper will focus on past drone attacks and activities by state and non-state actors across the globe and how the activities may lead to similar attacks on the agriculture sector within the next decade. The chapter concludes by recommending ways to strengthen defenses as well as topics for future research.

Growing Reliance on Drones in the Agriculture Industry

Globalization has led to the world's economies and agriculture industries becoming entwined, creating a powerful, interdependent system that has influenced global growth and development in positive and negative ways. Increased use of technological advancements in the agriculture and shipping industries has proven productive, increasing food production, storage, and shipping globally. The proliferation of unmanned systems and applications in the agriculture industry continues at an unprecedented scale, allowing farmers to increase overall yields while reducing resource consumption—commonly referred to as "precision agriculture." According to the Department of Homeland Security Office of Intelligence and Analysis 2018 Public-Private Analytic Exchange Program, "Precision agriculture employs a variety of embedded and connected technologies that rely on remote sensing, global positioning systems, and communication systems to generate big data, data analytics, and machine learning. These technologies allow for more precise application of agricultural and livestock management inputs such as fertilizer, seeds, and pesticides, resulting in lower costs and improved yields."[4] This convergence of technology and globalization in the agriculture sector increases exposure to and the risk of attacks from state and non-state actors in both the physical and virtual domains.

Recent technological developments in unmanned systems, data applications, and the Internet of things (IoT) continue to modernize the agriculture industry while increasing vulnerabilities in global food supplies. (The IoT refers to user or industrial devices [sensors, controllers, and household appliances] connected to the Internet and the network of devices that contain the hardware, software, firmware, and actuators that allow the devices to connect, interact, and freely exchange data and information.[5]) Improvements in computer technology, decreased manufacturing costs, and the miniaturization of components have enabled drone manufacturers to make more sophisticated unmanned systems cheaper for commercial use.[6] According to a December 2020 report published by Levitate Capital, "[t]he global drone economy will grow from $15B to $90B by 2030," with the most significant growth occurring within the logistics and enterprise markets.[7] The enterprise-drone market is composed of drone hardware, software, and service companies that create products for commercial and industrial applications.[8] The advent of the quadcopter and multicopter drones, which are highly versatile vertical takeoff and landing craft, has aided numerous commercial applications, ranging from filmmaking to agriculture.

The agriculture enterprise market is projected to undergo significant advancements over the next decade. In 2015, DJI, a China-based drone manufacturer and the world leader in civilian drones, established DJI Agriculture. This newly formed DJI subsidiary quickly became "a global leader in facilitating agricultural innovation through drone technology" that spans more than 100 countries located on six continents, according to the company's August 31, 2023, report.[9] The report explains that governments and farmers across the globe have adopted agricultural drones and smart-farming methods in a more scientific, sustainable, and eco-friendly way to increase food production. At the end of 2022, over 200,000 drones were operating across more than 200 million hectares globally.[10] (A hectare is equal to about 2.47 acres—the equivalent of two-and-a-half football fields.) A Grand View Research report states, "The US agriculture drone market size was estimated at USD 347.9 million in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 22.8% from 2023 to 2030."[11] The drone market's substantial compound annual growth rate mirrors the smart-retail market's projected growth from 2021–28, an expected valuation of $72.9 billion.[12] (The smart-retail market includes systems such as digital-signage solutions, smart labels, smart-payment systems, intelligent vending machines, augmented-reality solutions, virtual reality solutions, point-of-sale solutions, smart carts, robotics, and analytics.[13]) As more and more drones are put into service, the array of systems and applications needed to control them is also projected to rise.

Drone services and applications coupled with IoT technologies enable the agriculture sector to optimize. Monitoring farms manually that are spread over thousands of acres is challenging and costly, but recent technological solutions in high-speed Internet, smartphones, and cloud computing have provided farmers and ranchers innovative solutions. Cropin is an example of the agriculture industry's use of artificial intelligence (AI) and digitization to maximize visibility and revenue while minimizing risk and costs.[14] Cropin is an easy-to-use, seamless communication solution connecting growers, agribusinesses, and field officers and helping to digitize grower activities. Cropin serves as a farm-monitoring and management solution to help geotag farms, digitize farm and farmer records, share advisories, monitor crop productivity, improve farm efficiency, and boost field-officer productivity.[15] Cropin employs precision agriculture, drones, and digital-service applications to provide real-time solutions to the company's customers, increasing the demand for unmanned systems and applications within the sector. In 2015, DJI sought to capitalize on the thousands of drones its customers use by developing digital drone-application services that enable farmers to use IoT connectiveness with sensors, cameras, and data analysis services to enhance farming operations. For example, an industrial-scale Washington state potato

TOC

farmer reduced his insect damage by 80 percent through spot treatments using DJI-provided technology and services.[16] Each of these technologies provide businesses with significant capabilities, but each poses unique vulnerabilities and risks.

Threat Vectors

Although beneficial, the agriculture industry's digital revolution comes with consequences. According to a 2018 Department of Homeland Security report, "The adoption of advanced precision agriculture technology and farm information management systems in the crop and livestock sectors is introducing new vulnerabilities into an industry which had previously been highly mechanical in nature."[17] The associated risks these technologies pose to the agriculture sector increase the exposure to cyber and other related threats and vulnerabilities.[18] The report sheds light on some risks to confidentiality, integrity, and availability.

One of the confidentiality concerns is that major unmanned aircraft system "equipment manufacturers in the precision agricultural market are dominated by foreign built systems," allowing foreign governments unfettered access to collected sensor data.[19] Chinese manufacturer DJI is one example. Nathan Ord discusses the national security risks of foreign companies infusing IoT technologies into American companies and infrastructure.[20] Ord explains Chinese IoT cellular modules allow for remote data exploitation and the possibility of remotely terminating connected devices. To illustrate this point, in 2022, Russian troops overran a John Deere dealership in the Russian-controlled city of Melitopol, Ukraine, stealing 27 pieces of farm machinery worth $5 million.[21] The dealership was forced to access the stolen devices and disable them remotely, turning them into paperweights.

Threats to the integrity of agriculture sector data pose unique concerns. The intentional falsification of data through compromised information management systems and applications can have devastating effects on crops or livestock. For instance, animal diseases can wipe out herds or flocks, resulting in an immense economic toll and cascading consequences for food supplies. The Department of Homeland Security's 2018 research argues malicious actors' falsification of data to disrupt the agriculture industry is the highest-impact threat under the integrity standard.[22] Data falsification could have costly ramifications if false data is publicly released during an outbreak like the bird flu outbreak.

Incorrect information can result in increased response times and significantly delay efforts to rectify and resolve data discrepancies.

Agricultural operations ranging from farming to livestock heavily depend on equipment availability, which is extremely important for every crop sector because of the limited time windows for planting and harvesting. Equipment availability is critical during these times. For example, malevolent cyber actors could disrupt an entire fleet of unmanned agricultural devices, resulting in crops being ruined, or such actors could disable a poultry farm's climate-smart systems, resulting in unhealthy living conditions capable of spreading disease or causing death. In April 2023, Japan had to cull more than 17 million chickens due to a bird-flu outbreak, resulting in global price increases reaching historic high levels in the first quarter of 2023.[23] Despite this travesty having resulted from natural causes, the economic impacts and downstream consequences are still being felt today. The implications of a cyberterrorist-enabled attack of this magnitude would send shockwaves across the world.

The examples above are just a few ways precision-agriculture equipment can be compromised or exploited. The threat posed by foreign-supplied precision-agriculture equipment increases the likelihood that state actors and VEOs may seek to exploit these proverbial back doors surreptitiously to gain control of devices from afar or remotely disable them in bulk to impose economic costs and threaten food production.

Russia-Ukraine War: Agriculture at Risk

The Russia-Ukraine War has spurred the use of armed drones and their development to extraordinary levels. From the Iranian-made Shahed-136 suicide drones Russia uses to the Turkish-made TB2 drones Ukraine uses, these unmanned aerial vehicles (UAVs) have forever changed the battlefields of Eastern Europe.[24] The world has witnessed the destruction of thousands of acres of grain fields and storage silos located along the Black Sea by Russian drone strikes and ground forces. As of August 2023, Russia's successful drone attacks on Ukraine's grain-storage depots had destroyed over 270,000 metric tons of grain since Russia quit the Black Sea Grain Initiative in July 2023.[25] Russia's successful bombardment and grain ruination have been having catastrophic effects on Ukraine's agriculture sector, economy, and food security in a very short time frame. Ukraine's agriculture sector damages exceed $6.6 billion, but the total value of losses surpasses $34.25 billion, or 20–30 percent of the country's GDP.[26]

The inhabitants of the developing world are experiencing increased food shortages, surging prices, and fear as the war's disruptions spread.[27] Outside the conflict zone, 349 million people spanning 79 countries face acute food insecurity that will continue to worsen, with food supplies plummeting to a three-year low.[28] Many of the impoverished African, Middle Eastern, and Asian nations, which rely on Black Sea food supplies for their imports, are languishing from the global food crisis caused by the war in Ukraine.[29] The breadth and scope of the food-insecurity problem resulting from the Russia-Ukraine War highlight the grave impacts the conflict has had economically as well as on global food provisions and security.

In comparison, the American agriculture sector dwarfs that of Ukraine. In 2021, the United States had 895.3 million acres of farmland, whereas Ukraine cultivated around 40 million acres.[30] According to the US Department of Agriculture, a farm is "any place from which $1,000 or more of agricultural products were produced and sold, or normally would have been sold, during the year."[31] The department continues, "Government payments are included in sales. Ranches, institutional farms, experimental and research farms, and Indian Reservations are included as farms. Places with the entire acreage enrolled in the Conservation Reserve Program (CRP), Wetlands Reserve Program (WRP), and other government conservation programs are counted as farms."[32]

In 2021, US farm and food products contributed roughly $1.264 trillion (5.4 percent) of the America's overall $23.32 trillion gross domestic product.[33] Although the GDPs and agricultural production of the United States and Ukraine vary significantly, the threat to and impacts from attacks on this sector have far-reaching ramifications, as witnessed in the current conflict's impact on global food supplies. Imagine the ramifications of VEOs adopting similar attack methodologies: these attacks could threaten and cause immense damage to the American agriculture sector and economy.

Religiously Motivated Terrorists' Weaponization of Drones Threatens the Homeland

Religiously motivated terrorism is by far the largest and most impactful expression of extremism today. Groups like al-Qaeda, Hamas, Hezbollah, and the Islamic State in Iraq and Syria, which fall into this category, have used drones inside and outside conflict zones to conduct surveillance, gather intelligence, and perpetrate attacks. An *Air & Space Power Journal* article warns, "Violent nonstate actor drone use is more widespread, diverse, sophisticated, and rapidly advancing than depicted in the nascent literature" because "scholars have neglected or conflated commercial drones with military-grade platforms."[34] The Islamic State in Iraq and Syria used the DJI Phantom, a popular hobbyist model drone, in Iraq and the Levant region because this type of drone was inexpensive, available, and easy to use.[35] Access to low-cost drones has lowered the barriers to entry and given extremists a capability only nation-states could afford for years.

The proliferation of affordable commercial drones, which are more capable than hobbyist models and have larger carrying capacities, provides VEOs a more effective platform to use in future attacks.[36] The probability of VEOs weaponizing commercial drones over the next decade is extremely high due to commercial drones' pervasive growth across multiple sectors, ranging from agriculture to delivery services.[37] The days of VEOs needing to fundraise, purchase, or develop their own drone technology are a distant memory. Instead, extremists can leverage IoT connections and cyber-based capabilities to exploit and take control of commercial drones operating anywhere in the world. These drones lack the hardened security infrastructure of their counterparts in the defense sector. Even with these enhanced protections, VEO cyber actors can hack into military variants. As early as 2009, Iran-backed Iraqi militants hacked and took control of American military-drone video feeds.[38]

The FBI is concerned with the agriculture industry because it is one of the nation's 16 critical infrastructure sectors.[39] The incapacitation or destruction of one of these sectors could have debilitating effects that span from public health to national security. In 2021, the FBI notified agriculture cooperatives across the nation of various cyber-threat actors exploiting networks, systems, and application vulnerabilities within the food and agriculture sector.[40] In June 2023, the FBI's Omaha Field

Office identified four main cyber threats to the agriculture sector.[41] The first threat is from malicious cyber activities, such as ransomware or malware attacks, that can shut down agricultural operations. The second threat is theft of data or technology. China poses a significant threat in this arena. The third threat is countries, criminals, or terrorists trying to take control of agricultural processes, whether to stop or alter production, manipulate markets, or have an ecological effect. The final threat is the risk of bioterrorism or biowarfare, in which diseases or toxic agents are used to target food production. Each of these threat vectors can be exploited by terrorists seeking to attack the United States.

The following vignettes describe a few hypothetical attack vectors VEOs may use to target, exploit, and attack the US homeland using commercial agriculture drones in the not-so-distant future. As the digital environment pervades more and more aspects of human life, the attack surface for hostile activities in the virtual domain increases. Emergent technologies introduced into the crop and livestock sectors continue to create new vulnerabilities—especially, to cyber threats.[42] Most threats to precision agriculture's information management systems, applications, and technologies are from malicious actors seeking to steal, destroy equipment, or gain a competitive advantage by exploiting cyber-related vulnerabilities.[43] In 2020, a hacker disabled the computers at Pillen Family Farms in Nebraska, shutting down the entire genetic database and inhibiting the production of feed.[44] The attack affected nearly all activity for the agribusiness.

These same cyber-threat vectors afford VEOs the opportunity to have far-reaching consequences within the agriculture sector. In 2019, a group operating under the Islamic State in Iraq and Syria's hacking division announced a cyber campaign to target and destroy American websites, devices, and data in response to cybersecurity failures and vulnerabilities that a Senate report highlighted.[45] In a brazen cyberattack, the United Cyber Caliphate took down Pakistan International Airlines' website, paralyzing the airline's operations.[46] (The United Cyber Caliphate is a Southeast Asia–based hacktivist collective that has been responsible for distributed denial-of-service attacks and information leaks.[47])

Picture a large Midwestern precision-agriculture operation in the heartland of the United States. At the heart of the operation is an array of digital services, sensors, and unmanned systems interconnected by satellites, wireless signals, and web links. All digital components of the operation are extremely susceptible to cyberattacks, infiltration, and exploitation. What happens when these services cease to function? How is the food supply chain impacted? What is the economic fallout? A United Cyber Caliphate denial-of-service attack on the business's information management system could impact multiple interdependent industries simultaneously.

Remember the theoretical Midwestern farming operation and its IoT-connected sensors, applications, and array of unmanned systems. Imagine, for a moment, that an RMT group remotely accesses and takes control of the system. The group could extort the business owners for money, proprietary information and technology, or influence, or the group could disable or destroy the systems, rendering the equipment useless while crops wither away in the fields.

Agroterrorism is another threat vector that would have disastrous economic and psychological repercussions for the American agriculture sector and populace. (*Agroterrorism*, a subset of bioterrorism, is defined as "the deliberate introduction of an animal or plant disease for the purpose of generating fear, causing economic losses, or undermining social stability."[48]) A February 2021 Land Warfare Paper titled *The Role of Drones in Future Terrorist Attacks* concluded, "A particularly frightening application of drones is the distribution of chemical and biological agents, especially infectious diseases."[49] An attack of this caliber is by far the most dangerous but is unlikely due to the limited biowarfare-development capabilities terrorist groups like al-Qaeda and the Islamic State in Iraq and Syria possess. Toxic industrial chemicals and materials are readily available. An attack using chemicals like phosgene, chlorine, or a high-strength acid is within the realm of possibility and would have devastating consequences. For instance, an aerosolized pathogen, chemical agent, or toxic substance sprayed over America's largest concentrated animal-feeding operation (CAFO) in Grand View, Idaho, would devastate a company that had $4.5 billion in annual sales in 2020.[50] (Concentrated animal-feeding operations (CAFOs) are agricultural meat, dairy, or egg facilities where animals are kept and raised in confinement. Instead of grazing or eating in pastures or fields or on rangelands, animals are given food.[51]) The consequences of an agroterrorism attack—especially when considering associated industries and services (suppliers, transporters, distributors, and restaurant chains)—are unfathomable.[52]

Religiously motivated terrorists (RMTs) continue to refine their methods of delivering explosive-laden drones to their desired targets. Al-Qaeda and the Islamic State in Iraq and Syria's use of inexpensive and readily available drones, modified in makeshift facilities, has proven very effective in delivering grenades, mortars, and other improvised explosive devices.[53] Although these drones have proven effective, limited carrying capacity and range have restricted their use. With the commercialization of the agriculture industry, capacity and range are no longer constraints. Current agricultural drones can carry dry or liquid payloads ranging from a few ounces to hundreds of pounds of agricultural inputs, such as pesticides and fertilizer.[54] The Scorpion multicopter, a commercial drone, can carry a maximum payload of 1,000 pounds.[55] To compare, the MK-82 "500-pound bomb" dropped on Abu Musab al-Zarqawi contained 200 pounds of explosives.[56] Now picture an attack with an RMT-modified Scorpion laden with explosives and shrapnel on a high-capacity sporting event, critical-infrastructure location, CAFO facility, or other highly attended event or populated area. The impact of such a devastating attack would have cascading ramifications and economic costs. For example, an accidental fire at a CAFO facility in Texas caused an explosion that killed nearly 18,000 dairy cows in April 2023, affecting milk and hamburger production.[57] Think of the destruction a small kamikaze drone would cause if the drone were detonated inside one of these facilities; the carnage would be horrendous.

Similarly, the amount of damage insider threats can inflict is immense. Large farming operations rely heavily upon technological solutions such as drones and IoT-connected devices to reduce costs. Although these cost-saving measures provide the agriculture community with monetary savings, the measures pose an increased risk of exploitation and threats from within the homeland. Farmers in the United States are increasingly using foreign migrant workers to plant and harvest crops. Seventy percent of the nearly 2.4 million workers on farms and ranches in the United States in 2019–20 were foreign-born.[58] Radicalized migrant workers could leverage their placement and access within a large farming operation to acquire, modify, and employ unmanned systems easily or leverage the applications that control unmanned systems to commit an act of terrorism with deadly effects. Border agents in the United States have encountered or detained more than 563 individuals on terrorist watchlists while the individuals were entering the United States through its southern border this fiscal year.[59] Although this number is small in comparison to the number of illegal migrants entering daily,individuals with terrorist ties or affiliations are entering the porous US border. This phenomenon poses severe national security concerns. According to FBI Director Christopher Wray, "The primary terrorist threat to the homeland today, without question, is homegrown violent extremists"—that is, residents of the United States who are pursuing terrorist activity.[60] Self-radicalized or indoctrinated individuals seeking to support the Islamic State in Iraq and Syria, al-Qaeda, Hamas, or Hezbollah efforts inside the United States can quickly wreak havoc on the agriculture industry.

Keeping Food on America's Table

Creating a resilient agriculture industry is a must. Safeguarding agricultural operations from physical and virtual threats requires active security measures. The current US government structure perpetuates disorganized efforts to safeguard the nation's agriculture sector and economy from future terrorist events. The Department of Defense, the Department of Agriculture, the Department of Homeland Security, the Department of Health and Human Services, and the Environmental Protection Agency contribute to protecting the nation from terrorist groups that target the agriculture sector. Additionally, the Cybersecurity & Infrastructure Security Agency plays a pivotal role as a cybersecurity advisory agency. This agency provides education, alerts, and mitigation measures to US government organizations, commercial entities, and citizenry.[61] Consequently, the agency's reach into the private and commercial sectors is limited. The Cybersecurity & Infrastructure Security Agency relies on the Department of Defense and the FBI due to statutory limitations that restrict the agency's ability to confront cybercriminals, terrorists, and security organizations in a proactive, preventative manner.[62] The agency's lack of authority is a shortfall that should not persist if the US government is serious about protecting critical infrastructure from future drone- and cyber-related threats. Endorsement of the revisions prescribed in 6 US Code, section 124n, concerning the Department of Homeland Security's authority to address drone threats is crucial to protecting the homeland from emerging drone and cyber threats.[63] Despite robust government structures currently in position, the American agriculture industry is still a prime soft target for RMTs.

This chapter recommends three approaches to safeguarding agricultural operations from threats stemming from unmanned and related systems: vetting procedures, system redundancies, and proper cyber hygiene. First, instituting additional vetting and security measures for agricultural drone operators may help to dissuade would-be terrorists from venturing down the agroterrorism path. Ensuring employees are vetted and monitored for signs of radicalization would aid in identifying aspiring terrorists and preventing them from accomplishing their objectives. Establishing system redundancies would bolster the agriculture industry in the event of a terrorist attack in either the virtual or physical domain and make the sector more resilient. Within the cyber domain, cybersecurity and law-enforcement officials advocate for system administrators to remain vigilant, updating software- and hardware-security measures early and often. Educating workers and family members on how to protect company technology, identify signs of radicalization, and report concerns to the appropriate authorities is paramount to strengthening the industry's defenses. Responding to terror incidents requires a whole-of-societyapproach, like America's response to the September 11 attacks.

Due to the wide array of threats nation-states and non-state actors pose to the agriculture industry, several topics warrant future investigation. A close examination of state actors' use of technology to gain coercive control of other nations' agriculture industries is needed. The Chinese Communist Party's economic and technological investments in US agriculture are cause for concern.[64] Former US National Security Advisor H. R. McMaster testified to a congressional panel that the Chinese Communist Party "may be infiltrating Midwest US farm interests."[65] The economic consequences of this form of infiltration, exploitation, and coercion could make the economic impacts of the September 11 attacks pale in comparison. Legislative restrictions on the Chinese Communist Party and other nations' coercive activities are highly warranted. An investigation into the cybersecurity and defensive options the commercial industry could take to protect against pariah criminals and cyberterrorists is also necessary. The Cybersecurity & Infrastructure Security Agency's efforts are commendable, but without additional enforcement authority and capacity within the Department of Homeland Security and the FBI, commercial and agricultural businesses are left to protect their own assets, networks, and devices, creating vulnerabilities in America's national security, economy, and food supply. Lastly, the threat of other VEOs and lone wolves in the context of emerging technologies and homeland defense is significant. One individual with the right placement and access can strike a devastating blow within the US homeland.

Conclusion

Radical terrorism remains a persistent threat to the US homeland. The infusion of technology into the agriculture industry has proven invaluable for farmers and businesses, yet the vulnerabilities and risks the new technologies pose to global food supplies and the agriculture sector are frightening. The implications of terrorist attacks in this sector, ranging from agroterrorism and improvised drone attacks to crippling cyberattacks that can lead to devastating economic costs or increased food insecurity, are immense. Through education, awareness, and attentive security protocols and practices, the agriculture industry can remain informed, alert, and resilient in the face of terrorism. Although this paper focuses on attacks within the United States, the implications of such attacks far exceed US borders. Attacks on a country's agriculture industry have global implications, as witnessed in Ukraine. Members of NATO must review their internal security structures and practices and identify ways to make their agriculture industries more resilient to extremist attacks.

Endnotes

1. “Agricultural Drones Market Worth USD 24.9 Billion by 2030, at a CAGR of 29.30% by 2030 – Market Research Future (MRFR),” *GlobeNewswire* (website), May 24, 2023, https://www.globenewswire.com/en/news-release/2023/05/24/2675252/0/en/Agricultural-Drones-Market-Worth-USD-24-9-Billion-by-2030-at-a-CAGR-of-29-30-by-2030-Market-Research-Future-MRFR.html.

2. Jerrold M. Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to Al-Qaeda* (New York: Palgrave MacMillan, 2007).

3. Dean Olson, “Agroterrorism: Threats to America’s Economy and Food Supply,” FBI Law Enforcement Bulletin (website), February 1, 2012, https://leb.fbi.gov/articles/featured-articles/agroterrorism-threats-to-americas-economy-and-food-supply.

4. Larry Barrett et al., *Threats to Precision Agriculture* (Washington, DC: Department of Homeland Security, 2018), 3; and “Customs and Border Protection Enforcement Statistics,” US Customs and Border Protection (website), November 14, 2023, https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics.

5. “Internet of Things,” National Institute of Standards and Technology Computer Security Resource Center (website), n.d., accessed on September 12, 2023, https://csrc.nist.gov/glossary/term/internet_of_things.

6. Dario Constantine, *The Future of the Drone Economy* (Menlo Park, CA: Levitate Capital, December 11, 2020).

7. Constantine, *Drone Economy*, 2.

8. Richard J. Gross, “Complete Evolution and History of Drones: From 1800s to 2023,” Propel RC (website), May 11, 2023, https://www.propelrc.com/history-of-drones/.

9. “New DJI Agriculture Drone Insight Report Reveals Greater Acceptance, Advanced Farming Techniques, and Exploration of Best Practices for Farmers,” DJI Agriculture (website), August 31, 2023, https://ag.dji.com/newsroom/ag-news-en-insight-report-2022.

10. “Drone Insight Report.”

11. Grand View Research, *US Agriculture Drone Market Size, Share & Trends Analysis Report by Type (Fixed Wing, Rotary Wing), by Component (Hardware, Software, Services), by Farming Environment, by Application, and Segment Forecasts, 2023–2030* (San Francisco: Grand View Research, August 2023).

12. Zion Market Research, “At 22.8% CAGR, Smart Retail Market Size & Share to Hit USD 72.9 Billion, Globally by 2028, Says Zion Market Research—Smart Retail Industry Trends, Growth, Value, Analysis & Forecast Report,” PR Newswire (website), June 21, 2022, https://www.prnewswire.com/news-releases/at-22-8-cagr-smart-retail-market-size--share-to-hit-usd-72-9-billion-globally-by-2028--says-zion-market-research--smart-retail-industry-trends-growth-value-analysis--forecast-report-301572019.html

13. Zion Market Research, “Smart Retail Market Size.”

14. “Every Pixel Tells a Story,” Cropin (website), n.d., accessed on September 4, 2023, https://www.cropin.com/.

15. “Every Pixel.”

16. “Drone Insight Report.”

17. Barrett et al., *Threats to Precision Agriculture*, 3; and “Enforcement Statistics.”

18. Barrett et al., *Threats to Precision Agricultur*e; and “Enforcement Statistics.”

19. Barrett et al., *Threats to Precision Agriculture*, 4; and “Enforcement Statistics.”

20. Nathan Ord, “Chinese Cellular IoT Radio Modules Pose an Alarming US National Security Risk,” Hot Hardware (website), August 30, 2023, https://amp.hothardware.com/news/chinese-manufactured-iot-cellular-modules-pose-national-security-risk.

21. Peter Holderith, “John Deere Tractors Stolen by Russia in Ukraine Remotely Disabled,” Drive (website), May 3, 2022, https://www.thedrive.com/news/john-deere-tractors-stolen-by-russia-in-ukraine-remotely-disabled.

22. Barrett et al., *Threats to Precision Agriculture*; and “Enforcement Statistics.”

23. Michelle Toh, "Japan Is Running Out of Space to Bury Chickens Culled over Bird Flu," *CNN Business* (website), April 6, 2023, https://www.cnn.com/2023/04/06/business-food/japan-bird-flu-land-shortage-intl-hnk/index.html.

24. Isabelle Khurshudyan, Mary Ilyushina, and Kostiantyn Khudov, "Russia and Ukraine Are Fighting the First Full-Scale Drone War," *Washington Post* (website), December 2, 2022, https://www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/.

25. Miranda Nazzaro, "Russia, Ukraine Trade Drone Attacks," *Hill* (website), August 23, 2023, https://thehill.com/policy/international/4166478-russia-ukraine-trade-drone-attacks/.

26. Caitlin Welsh, "Russia, Ukraine, and Global Food Security: A One-Year Assessment," Center for Strategic and International Studies (website), February 24, 2023, https://www.csis.org/analysis/russia-ukraine-and-global-food-security-one-year-assessment.

27. Franco Ordoñez, "Russian Wreak Havoc on Ukrainian Farms, Mining Fields and Stealing Equipment," NPR (website), May 6, 2022, https://www.npr.org/2022/05/06/1096481280/ukraine-agriculture-farms-russia-war.

28. Georgieva, "Joint Statement."

29. Welsh, "Global Food Security."

30. Rob Cook, "Ranking of States with the Most Land in Farms," Beef2Live (website), updated December 22, 2023, https://beef2live.com/story-states-land-farms-ranking-1-50-90-113145.

31. Cook, "Ranking of States."

32. US Department of Agriculture, *Farms and Land in Farms: 2021 Summary* (Washington, DC: US Department of Agriculture, February 2022), 14.

33. "U.S. GDP 1960–2023," Macrotrends (website), n.d., accessed on December 15, 2023, https://www.macrotrends.net/countries/USA/united-states/gdp-gross-domestic-product; and "Ag and Food Sectors and the Economy," Economic Research Service (website), updated November 3, 2023, https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and-the-economy/.

34. Ori Swed and Kerry Chavez, "Off the Shelf: The Violent Nonstate Actor Drone Threat," *Air & Space Power Journal* (Fall 2020): 30, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf.

35. Swed and Chavez, "Off the Shelf," 29–43.

36. Swed and Chavez, "Off the Shelf," 29–43.

37. Pamela Cohn et al., "Commercial Drones Are Here: The Future of Unmanned Aerial Systems," McKinsey and Company (website), December 5, 2017, https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems.

38. Steven Stalinsky and R. Sosnow, "A Decade of Jihadi Organizations' Use of Drones – From Early Experiments by Hizbullah, Hamas, and Al-Qaeda to Emerging National Security Crisis for the West as ISIS Launches First Attack Drones," Middle East Media Research Institute (website), February 21, 2017, https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda.

39. "Critical Infrastructure Sectors," Cybersecurity & Infrastructure Security Agency (CISA) (website), n.d., accessed on November 24, 2023, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

40. FBI, *Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons*, Private Industry Notification no. 20220420-001 (Washington, DC: FBI, April 20, 2021).

41. Martha Stoddard, "Criminals, Terrorists, Hostile Foreign Powers Targeting Nebraska Agriculture, FBI Warns," *Lincoln Journal Star* (website), June 8, 2023, https://journalstar.com/news/state-regional/business/article_ccce4b85-ef3c-5e83-8340-05d026489a1a.html.

42. Barrett et al., *Threats to Precision Agriculture*; and "Enforcement Statistics."

43. Barrett et al., *Threats to Precision Agriculture*; and "Enforcement Statistics."

44. Stoddard, "Criminals, Terrorists."

45. Bridget Johnson, "New ISIS Cyber Campaign Announced as Supporters Share US Agency Vulnerabilities," Homeland Security Today (website), July 1, 2019, https://www.hstoday.us/subject-matter-areas/cybersecurity/new-isis-cyber-campaign-announced-as-supporters-share-u-s-agency-vulnerabilities/.

46. "ISIS-Linked Hackers Ground Pakistan's National Airline Website," Times Now (website), April 2, 2023, https://www.timesnownews.com/technology-science/isis-linked-hackers-ground-pakistans-national-airline-website-article-99184088.

47. "ISIS-Linked Hackers."

48. Olson, "Agroterrorism."

49. Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, Land Warfare Paper no. 137 (Arlington, VA: Association of the US Army, February 2021), 7.

50. "The Biggest CAFO in the United States," *Wickersham's Conscience* (blog), March 20, 2020, https://wickershamsconscience.wordpress.com/2020/03/20/the-biggest-cafo-in-the-united-states/.

51. "Environmental Health: Concentrated Animal Feeding Operations (CAFOs)," Wisconsin Department of Health Services (website), February 6, 2023, https://www.dhs.wisconsin.gov/environmental/cafo.htm.

52. Peter Chalk, *Agroterrorism: What Is the Threat and What Can Be Done about It?*, RB-7565-OSD (Santa Monica, CA: RAND Corporation, 2003).

53. Ryan Jokl Ball, *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications*, LLNL-TR-740336 (Livermore, CA: Lawrence Livermore National Laboratory, October 17, 2017); and Mahmut Cengiz, "Prevention of the Procurement of Arms and Explosives by Terrorist Groups," in *Handbook of Terrorism Prevention and Preparedness*, ed. Alex P. Schmid (The Hague: International Center for Counter-Terrorism, 2021).

54. Jack Crawford, "What Is the Biggest Farm Drone?," Farms Wise (website), n.d., accessed on September 8, 2023, https://farmswise.com/the-biggest-farm-drone/.

55. "Full Throttle Aerial Scorpion," Electric Vertical Takeoff and Landing News (website), n.d., accessed on September 1, 2023, https://evtol.news/full-throttle-aerial-scorpion.

56. Daniel Engber, "How Heavy Is a 500-Pound Bomb?," *Slate* (website), June 9, 2006, https://slate.com/news-and-politics/2006/06/how-heavy-is-a-500-pound-bomb.html.

57. Jayme Lozano Carver, "Here's How the Fire That Killed Nearly 18,000 Texas Cows Got Started," *Texas Tribune* (website), May 19, 2023, https://www.texastribune.org/2023/05/19/cows-dairy-farm-texas-investigation/.

58. Department of Labor, *Findings from the National Agricultural Workers Survey (NAWS) 2019–2020: A Demographic and Employment Profile of United States Farmworkers*, Research Report no. 16 (Washington, DC: Department of Labor, January 2022).

59. Julia Ainsley, "Number of People on Terrorist Watchlist Stopped at Southern US Border Has Risen," *NBC News* (website), September 14, 2023, https://www.nbcnews.com/politics/national-security/number-people-terror-watchlist-stopped-mexico-us-border-risen-rcna105095.

60. Christopher Wray, "Countering the Terrorist Threat through Partnerships, Intelligence, and Innovation" (speech, Utah National Security and Anti-Terrorism Conference, Salt Lake City, UT, August 29, 2018), https://www.fbi.gov/news/speeches/countering-the-terrorist-threat-through-partnerships-intelligence-and-innovation.

61. "Cybersecurity Alerts & Advisories," CISA (website), n.d., accessed on November 24, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories.

62. Marisol Cruz Cain and Gretta L. Goodwin, *CYBERCRIME: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics*, GAO-23-106080 (Washington, DC: Government Accountability Office, June 2023).

63. Protection of Certain Facilities and Assets from Unmanned Aircraft, 6 U.S.C. § 124n (2018).

64. Lauren Greenwood, *China's Interests in US Agriculture: Augmenting Food Security through Investment Abroad* (Washington, DC: US-China Economic and Security Review Commission, May 26, 2022).

65. OneAdmin, "China May Be Infiltrating American Ag Interests, Says Former US National Security Advisor," *Hoosier Ag Today* (website), March 5, 2023, https://www.hoosieragtoday.com/2023/03/05/china-may-be-infiltrating-american-ag-interests-says-former-us-national-security-advisor/.

– 4 –

Spatial Anchors and Dangerous Liaisons: Terrorist Collaboration in an Augmented Age

Kristan J. Wheaton

Over the next five to 10 years, augmented reality (AR) tools are highly likely to enable terrorist networks to collaborate across borders in new ways that will be difficult to detect or prevent. AR technologies like smart glasses will allow users to overlay digital images onto the real world, creating virtual experiences. Terrorists will likely use AR to travel to and inside foreign countries to meet with collaborators in impactful, quasi-physical ways without documentation.

Augmented reality will also likely enable terrorist recruiters worldwide to connect through digital markers—so-called "spatial anchors"—in the real-world environment. Recruiters can evaluate recruits through an AR analysis of their digital footprints, avoiding risky in-person meetings. Augmented reality can also help terrorists to plan operations remotely by digitally monitoring locations and even potentially executing attacks while avoiding physical surveillance.

As AR develops, terrorists will likely leverage its borderless nature for recruitment, planning, and communications in hard-to-detect ways, such as encrypted AR apps tailored to different users that provide detailed maps and communications. Agencies must understand AR developments to prevent terrorist exploitation before it becomes reality. With vigilance and cooperation, the most dangerous uses of AR may be prevented. But the rise of AR requires a global response to this new terrorist threat that transcends borders.

Augmented Reality Technology Today

A young man walks down a busy city street. His jeans and windbreaker make him look like every other young man in the city, yet his backpack marks him as a student. He seems alone, but his lips are quietly moving as he navigates through the crowds. If you could get close enough to him, you would barely hear his side of an anxious conversation.

He stops to shift the weight of his backpack. The backpack is heavy and uncomfortable, but his eyes, visible through his glasses, maintain their point of focus, as if he is looking at something or listening to someone two feet to the right. Just five years ago, in 2025, such behavior would have seemed odd and out of place, but today, a casual survey of the people walking down the same street reveals several similarly quiet conversations taking place. Indeed, people have given this particular activity a name: specspeak.

According to Microsoft, AR is "an enhanced, interactive version of a real-world environment achieved through digital visual elements, sounds, and other sensory stimuli via holographic technology."[1] Today, AR applications reside primarily on smartphones and tablets. These applications allow users to overlay digital information onto the real world. In some cases, as with the game *Pokémon GO*, applications allow players to interact with cartoon characters anywhere and at any time. Other applications, such as Google's Live View feature in Google Maps, gives users clear paths to their destinations laid on top of the real world and visible through the windows of their phones or tablets. Just as AR technologies enhance the lives of users, these technologies will be available to terrorist organizations for recruitment, indoctrination, planning, and operations.

Several technologies support the current generation of AR, and they are virtually certain to be important as technology improves over the next 10 years. The Global Positioning System is the most obvious, with its constellation of satellites allowing for precise positioning on Earth. The Global Positioning System supports spatial anchoring, a particularly important component of most AR systems that permits digital objects to be anchored to a physical location and tracked over time. Other technologies, such as AI–enabled facial recognition and lidar point-cloud generation, support AR applications designed to operate near users (such as Snapchat filters).

But all current AR applications suffer from three issues: bandwidth limits, narrow fields of view, and mobile-phone distraction. Many of the most useful AR applications require users to be able to move. Thus, AR depends on the capabilities of local mobile networks. Although data throughput has advanced rapidly over the last 20 years—from about 300 kilobytes per second over 3G, basic networks to more than one gigabyte per second over the fastest 5G networks—this throughput is still insufficient for realistic, real-time, three-dimensional video, particularly while moving.[2]

Moreover, typical smartphone cameras can only see about 72 of the 360 degrees that surround users. Wide-angle and fish-eye lenses can push this number up to 160 degrees with some inevitable distortion.[3] This narrow field of view makes losing spatially anchored digital items easy because they quickly float off-screen.[4]

Mobile-phone distraction, in which users are so focused on their phones they lose track of events happening in the surrounding environment, is familiar to everyone in one form or another. Within the context of AR, however, mobile-phone distraction is particularly problematic. To engage with or even see an AR image, users must be focused almost exclusively on their mobile devices.[5] This effect is even more distracting when the AR image is interactive.

Developers are well aware of these issues and hard at work solving them. Indeed, all challenges to widespread AR adoption are likely to fade over the next 10 years as 6G networks come online and the primary user interface moves from a handheld phone to a hands-free pair of smart glasses.

Network providers and manufacturers are already heavily researching 6G, which is a natural progression from the current 5G networks. Currently, most telecommunications experts see 6G coming online around 2030.[6] Explicitly designed to make the distinction between physical and digital appear seamless, 6G promises terabyte-per-second speeds, or 10 times the speed 5G currently provides.[7]

The move from handheld devices to smart glasses is happening even more quickly. The announcement of the Apple Vision Pro headset in early 2023, with its focus on so-called "calming technology" designed to make Apple's products natural and easy to use, in early 2023 is a prime example of a broader trend.[8] Microsoft, which continues to promote its HoloLens AR product, as well as Meta, Google, and other large technology

TOC

companies are participating in this trend. These companies are funding the development of a wide variety of AR-enabled glasses. Over time, as software and hardware improve, these glasses will solve the problems of field of view and mobile-phone distraction by placing a personal, editable, mostly transparent heads-up display in front of the users' eyes, leaving their hands free and reducing distractions.

One final technology is required to enable the vision of an AR-enhanced future: batteries. Storage capacity for batteries increased 85 percent between 2011 and 2021, and the United States has set the goal of further reducing battery production costs from the current $143 per kilowatt-hour to just $60 per kilowatt-hour by 2030.[9] Similar efforts are underway in China, European nations, and other technologically sophisticated countries. These improvements will allow AR-enabled glasses to work longer, weigh less, and provide a better user experience than is available presently.

Near-Future Improvements in Augmented Reality

"I don't feel worthy," says the young man as he looks down. He hears a soft laugh, an old man's laugh he had heard many times before. "We are all worthy, my son," says a deep, calming voice.

The young man looks up and to the right. He can see the old man—his long beard and flowing hair, his tattered robe, and his piercing blue eyes—as well as his smile. The young man has watched so many videos of this old man speaking the plain truth to people around the world. The young man was nervous when he first reached out, looking for more information, but he was immediately welcomed into a virtual-reality session inside the leader's home. Many more meetings followed, but these sessions had always been in large groups or with other members of the movement. Today, on the young man's own street, in his own city, the leader is walking with him. Just him.

In the middle of a crowded plaza, the young man spots a bench and walks toward it. "Brother John said this was the best place," he says to the leader.

"Brother John is a good man," replies the leader. "I'm glad you had the chance to know him."

The young man sheds his heavy backpack and sets it carefully beside him as he sits down. He, with Brother Edward's help, had built and packed everything inside it. The young man knows how dangerous the backpack is.

Still, he is comforted by the fact the same technology that allows him to speak with the leader also protects the leader, Brother John, and Brother Edward from the local police and their network of informants.

Along with the arrival of novel technologies, incremental improvements in other, more traditional technologies—encryption and social media, in particular—will increase the difficulty of preventing or even observing terrorist activities conducted with AR-enabled devices. Law-enforcement agencies and legislation will likely struggle to keep apace.

The war between coders and code breakers has persisted since ancient times. Today, in the United States, the National Institute of Standards and Technology oversees eight projects designed to improve on current cryptographic standards. These projects include efforts in postquantum cryptography, block ciphers, and random-bit generation.[10] Even if cracking codes that are generated using these improved cryptographic standards is theoretically possible, advanced encryption algorithms will inevitably provide powerful protection against underfunded law-enforcement efforts over operationally relevant time frames.

As social media evolves to take advantage of AR-enabled devices and capabilities, a proliferation of new and existing networks will likely make tracking AR interactions increasingly difficult. Currently, at least 35 social-media networks have over 100 million active users.[11] This number does not include other services with many of the same communication features as social media, such as Zoom or FaceTime. Nor does the number include gaming-support platforms such as Discord or Twitch or even the games themselves, which often come with built-in communication technologies for collaborative play.

The risk associated with the virtual worlds created by both social media and games is well understood by the US intelligence community. As far back as 2008, the US intelligence community warned about the possibilities of virtual worlds: "It is likely that adversaries increasingly will use virtual worlds to engage in propaganda, recruitment, coordination, training, and information gathering. Because of the immersive nature of the experience, virtual worlds are a particularly powerful medium to influence behavior, including offline behavior. The online experiences that users carry back to the real world will be subject to manipulation and influence."[12]

A follow-up report in 2009 stated, "The current state of knowledge, at least among the LE [law enforcement] community, is insufficient to address these issues in any meaningful way"—a situation that likely persists in most jurisdictions.[13]

Psychological Impact of Augmented Reality

The young man shifts his weight on the bench and looks around the plaza, which is crowded, but he knew it would be this time of day. "So many children," he says in a soft voice, as if to himself.

"What is rule number two?" asks the old man.

The young man turns toward the stern face and piercing, blue eyes of the leader. "The children of my enemy are my enemy," says the young man, his conviction renewed.

On some level, the young man knows the leader is just a hologram, a digital version of the leader projected with hyperrealistic accuracy onto his glasses. But it doesn't feel that way. The young man feels as though he matters. More importantly, the young man is inspired by his leader's presence, by his willingness to accompany the young man on the mission.

"It's time," says the old man finally.

The young man knows what to do. He reaches into the backpack and flips three switches, in the exact order he has been taught. "There, the task is done," he thinks. The young man knows he has to stay. He knows an unattended backpack would be spotted immediately. He sighs and turns to the old man. "Stay with me," he asks.

The old man looks at him with love and kindness. "Do you remember the first song you were taught?"

"The song of the Tribe?" the young man responds, a little uncertain.

"Yes, that one. Sing it with me now."

Although the wide range of technological advancements over the next 10 years is highly likely to facilitate terrorist operations, the most profound effect of this convergence may be psychological. Although much of the research into the emotional impact of virtual reality and AR is new and quickly evolving, the research tends to suggest users interpret virtual experiences as if they are real and happening to the users personally. Combined with older literature on obedience and proximity, the research implies virtual authority figures will have the same emotional impact on people as real ones often do.

The earliest studies of obedience are, of course, those performed by Stanley Milgram in 1963. In these well-replicated studies, Milgram found many subjects obeyed authority figures, even when the figures asked the subjects to perform questionable acts. Furthermore, Milgram found the proximity of the authority figure increased the participants' obedience.[14]

More recent experiments found these same effects exist in virtual environments as well. In 2006, for example, researcher Mel Slater from University College London replicated the Milgram experiments using a virtual human. Slater found that "in spite of the fact that all participants knew for sure that neither the stranger nor the shocks were real, the participants who saw and heard her tended to respond to the situation at the subjective, behavioural and physiological levels as if it were real."[15] More recently, Verity McIntosh from the University of the West of England tested subjects in realistic training simulations, finding "participants overall demonstrate high levels of 'perceptual proximity' to the experience, recounting it as something that happened to them directly and personally."[16]

Diminished Physical Presence, Heightened Virtual Threat

Additional research needs to be conducted, but, if confirmed, these results suggest the hyperrealistic AR forecasted in this chapter and elsewhere has significant implications for counterterror operations. In short, if leaders of terrorist organizations can recruit, indoctrinate, plan, and operate using AR with little drop-off in effectiveness while staying safely in hiding, the challenges faced by national security and law-enforcement organizations will increase exponentially.

Nothing but static is on the screen in front of the old man now. The old man stands up and takes off his robe. The beard was digital, of course, but he wears the robe because, as bulky and scratchy as it is, he thinks it looks more authentic.

He takes a quick look around the room. He isn't worried; he knows a crew will clean the room soon, destroying all evidence that he had ever been there. "Another drone successfully launched," he thinks as he leaves the room, closing the door behind him. Out on the street, he turns toward a local bar. He wants to see what the news has to say before he files his report.

Endnotes

1. “What Is Augmented Reality or AR?,” Microsoft Dynamics 365 (website), n.d., accessed on August 31, 2023, https://dynamics.microsoft.com/en-us/mixed-reality/guides/what-is-augmented-reality-ar/.

2. “Download Speeds: What Do 2G, 3G, 4G, and 5G Actually Mean?,” Ken’s Tech Tips (website), November 23, 2018, https://kenstechtips.com/index.php/download-speeds-2g-3g-and-4g-actual-meaning.

3. Jianxun Chu et al., “Attention or Distraction? The Impact of Mobile Phone on Users’ Psychological Well-Being,” *Frontiers in Psychology* 12 (April 2021): https://doi.org/10.3389/fpsyg.2021.612127.

4. Stan Kurkovsky et al., “Current Issues in Handheld Augmented Reality,” in *2012 International Conference on Communications and Information Technology* (New York: Institute of Electrical and Electronics Engineers, 2012).

5. Arjun Kharpal, “Next-Gen Mobile Internet – 6G – Will Launch in 2030, Telecom Bosses Say, Even as 5G Adoption Remains Low,” *CNBC* (website), March 7, 2023, https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html.

6. “Follow the Journey to 6G,” Ericsson (website), n.d., accessed on August 31, 2023, https://www.ericsson.com/en/6g.

7. “Follow the Journey.”

8. “Apple Vision Pro,” Apple (website), n.d., accessed on August 31, 2023, https://www.apple.com/apple-vision-pro/; and Helen Papagiannis, “Calm Technology and the Future of Augmented Reality,” World Economic Forum (WEF) (website), August 18, 2023, https://www.weforum.org/agenda/2023/0/calm-technology-future-of-augmented-reality/.

9. Department of Energy, *Executive Summary: National Blueprint for Lithium Batteries 2021–2030* (Washington, DC: Department of Energy, June 2021).

10. “Cryptography,” National Institute of Standards and Technology (website), n.d., accessed on December 22, 2023, https://www.nist.gov/cryptography.

11. *Wikipedia*, s.v. “List of Social Platforms with at Least 100 Million Active Users,” updated September 1, 2023, https://en.wikipedia.org/w/index.php?title=List_of_social_platforms_with_at_least_100_million_active_users&oldid=1173223873.

12. Office of the Director of National Intelligence (ODNI), *3D Cyberspace Spillover: Where Virtual Worlds Get Real* (Washington, DC: ODNI, 2008).

13. ODNI, *Mixed Reality: Geolocation and Portable Handheld Communication Devices* (Washington, DC: ODNI, 2009); and Mark A. Lemley and Eugene Volokh, “Law, Virtual Reality, and Augmented Reality,” *University of Pennsylvania Law Review* 155, no. 5 (April 2018): 1051–138, https://scholarship.law.upenn.edu/penn_law_review/vol166/iss5/1.

14. Jerry M. Burger, “Conformity and Obedience,” Noba (website), n.d., accessed on September 1, 2023, https://nobaproject.com/modules/conformity-and-obedience.

15. Mel Slater et al., “A Virtual Reprise of the Stanley Milgram Obedience Experiments,” *Public Library of Science ONE* 1, no. 1 (December 2006).

16. Verity McIntosh, “Dialing Up the Danger: Virtual Reality for the Simulation of Risk,” *Frontiers in Virtual Reality* 3 (2022): https://doi.org/10.3389/frvir.2022.909984.

— 5 —

Emerging Biotechnology Capacity and Emerging Biosecurity Threats in Colombia and Chile

Steve S. Sin, PhD

Introduction

With the onset of the COVID-19 pandemic, countries around the world came to recognize the importance of maintaining a national stockpile of biologics (for example, vaccines) and, if possible, possessing domestic capabilities to produce the biologics required to fight the spread of communicable diseases. In South America, Colombia and Chile at one point possessed robust vaccine production capabilities but abandoned them decades ago.[1] Although some within these countries called for a renewal of their vaccine production capabilities, the calls went unheard—that is, until the COVID-19 pandemic. As the world weathered the pandemic and countries scrambled to secure the vaccines needed to combat it, Colombia and Chile decided they would return to producing biologics domestically as well as double down on their already-active biotechnology policies that had been designed to encourage public-private partnerships and attract foreign investments.[2]

With the fast pace of advancements in biotechnology, and as Colombia and Chile continue to develop their biotechnology capacities, the potential for biosecurity threats in these countries is increasing. By analyzing terrorist and insurgent threats as well as the biosecurity legal frameworks of Colombia and Chile, this research paper assesses the potential emerging threats and provides recommendations on activities NATO could implement to mitigate these emerging threats.

Violent Non-state Actor Use of Biological Agents

Fiction

A scientist steals the prototype of a programmable, deoxyribonucleic acid–targeting nanobot bioweapon from a government laboratory, operationalizes the weapon, and provides it to a transnational, hybrid criminal-terrorist organization. This organization deploys the bioweapon at several public events across the country, targeting specific people attending these events. Working as designed, the bioweapon infects only the intended targets, leaving others who were also exposed to the bioweapon unaffected. A few days after deployment, several emergency rooms across the country start receiving patients who are extremely ill with no apparent explanations. Finally, all patients die within a few days of being admitted to the hospital. No other patients exhibiting the same symptoms are admitted to any hospitals in the country after this single wave of incidents. Although the country's public health apparatus attempted to trace the source of these seemingly unrelated yet oddly congruent events, the apparatus was not successful in doing so, and the incidents remain a mystery—that is, of course, until the hybrid criminal-terrorist organization in question decides to deploy the bioweapon on another set of targets.

Emerging Technology and Threat

You may think the scenario presented above reads like a spy-thriller movie, complete with a sophisticated and well-resourced, transnational criminal-terrorist organization; an element of an insider threat in the form of a government scientist who turns bad; and a futuristic bioweapon that is deadly only to its intended targets. The scenario is part fiction; the author constructed it based on the premise for the bioweapon technology (and its acquisition path) that appears in the 2021 James Bond movie *No Time to Die*. The scenario above illustrates what captures imaginations when people think about bioterrorism and emerging technology. Of course, advances in biomedical and bioengineering technologies over the past decade as well as their continued advancements make the scenarios like the one described above not too far-fetched. Do-it-yourself clustered regularly interspaced short palindromic repeat (DIY CRISPR) kits, plastic-eating enzymes, and gene-targeting therapies are but a few examples of recent biomedical and bioengineering advancements witnessed in the real world that make the fantastical scenarios written for the movies seem realistic, rather thanmerely feasible and plausible. Take the DIY CRISPR kit, for example: Security experts have pointed out numerous times that this technology is an example of a bioengineering advancement that could potentially pose a threat, especially in the hands of violent non-state actors (VNSAs).[3] Although this assessment is certainly well founded, the empirical data on VNSA pursuit and use of biological agents (and bioweapons) thus far paints a slightly different picture.

Data

The Violent Non-State Actor Chemical, Biological, Radiological, and Nuclear Event Database, maintained by a research team at the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism, headquartered at the University of Maryland, is an open-source database that contains 565 chemical, biological, radiological, and nuclear events planned or perpetrated by ideologically motivated VNSAs that occurred between 1990 and 2022. According to the database, of the 565 chemical, biological, radiological, and nuclear events, 123 (21.8 percent) were classified as biological. Of those events, 66 involved toxins (53.7 percent of biological events or 11.7 percent of all events in the database) and 57 involved biological agents (46.3 percent of biological events or 10.1 percent of all events in the database). Most toxin events involved ricin (49 incidents or 74.2 percent of all toxin events). The most prevalent biological agent events involved the anthrax bacterium *Bacillus anthracis* (18 incidents or 31.6 percent of all biological agent events). Finally, regardless of the agent pursued, none were acquired using emerging biomedical or bioengineering technologies or techniques.[4]

For South America specifically, the database records 17 total chemical, biological, or radiological incidents, all of which occurred between 1998 and 2005. Of these 17 incidents, four are classified as biological incidents: two in 2003 (one in Trinidad and Tobago and one in Brazil) and two in 2005 (both in Colombia). Figure 5-1 provides a summary of four biological incidents that occurred in South America that are included in the database.[5]

Table 5-1. Summary of biological incidents in South America and the Caribbean, 1990 to present

On January 26, 2003, the *Trinidad Express* reported on an interview the newspaper had conducted with an unnamed terrorist group in Trinidad. The terrorist group claimed it was preparing unspecified chemical and biological weapons for retaliatory attacks against US and British interests in the event the United States and United Kingdom invaded Iraq. The unnamed terrorist group showed the newspaper various purported chemicals during the interview. According to the Caribbean Media Corporation, the Trinidad and Tobago Forensic Science Center rebuffed the news report, saying most of the items identified in the lab were not able to produce biological weapons

According to *Agência Estado*, on September 12, 2003, an employee at the US consulate in São Paulo, Brazil, opened an envelope that contained an unspecified white powder. According to *Agência Estado* and *Folha de Sao Paulo*, the employee had an allergic reaction to the substance, went to the hospital, and was released the same day.

On August 10, 2005, a Colombian National Army official announced the seizure of 1,200 pounds of cyanide-laced bullets from the Revolutionary Armed Forces of Colombia (FARC) in Labranzagrande, Colombia. In addition to the cyanide-laced bullets, Colombian authorities seized an unspecified number of bullets that were coated in fecal matter, according to *El Espectador*.

In early August 2005, members of the Popular Liberation Army attacked police officers with cyanide-coated bullets and fecal matter–coated bullets. Four Colombian police officers died in the attack, *El Colombiano* and *El Tiempo* reported.

One can glean from the summaries that these incidents were not sophisticated, and they certainly did not involve the use of any advanced biotechnology.

Terrorist and Insurgent Threats

Colombia

Colombia has a long history of internal violence in the form of insurgency and terrorism that was significantly reduced following the agreement and implementation of the 2016 Peace Accord. Despite the agreement, the frequency of violence continues to increase.[6]

Terrorist/Insurgent Groups

Although the Revolutionary Armed Forces of Colombia formally dissolved after the 2016 Peace Accord with the Colombian government and the United States removed the group from the Foreign Terrorist Organizations list in 2021, FARC dissident groups that refused the peace agreement continue to operate, with the Ejército de Liberación Nacional (National Liberation Army) among the primary domestic terrorist and insurgent groups operating within Colombia.[7] As such, the United States has designated the Revolutionary Armed Forces of Colombia's two main dissident groups—the FARC People's Army and its rival, Segunda Marquetalia—as foreign terrorist organizations.[8] The National Liberation Army and these FARC dissident groups maintain areas of influence in Colombia, and their activities extend across borders into Venezuela.[9] Table 5-2 lists Colombia's currently active terrorist and insurgent groups; in this context, biosecurity relevance is based on whether the group has undertaken attacks against biosecurity infrastructure or demonstrated interest in the pursuit or use of biological agents as weapons.

Table 5-2. List of active domestic terror or insurgent groups in Colombia

Group	Activity	Incident	Still Active?	Biosecurity Relevance
FARC People's Army	Insurgency/ guerilla actions/ abductions		Yes	No
Segunda Marquetalia	Insurgency/ guerilla actions		Yes	No
National Liberation Army	Bombing/ explosives	Detonated an explosive device at Ecopetrol's Caño Limón – Coveñas and Transandino oil pipelines; attributed though not claimed attacks.	Yes	No
National Liberation Army	Bombing/ explosives	A suicide bomber detonated an explosive device–laden vehicle at a police station, killing 22 (including the assailant) and injuring 67.	Yes	No

Terrorist/Insurgent Incidents since 2010

Conventional

The 2016 Peace Accords between the Colombian government and the Revolutionary Armed Forces of Colombia brought a brief decline in terrorist and insurgent incidents in Colombia. Since 2016, Colombia has faced a continuous rise in incidents. Since 2019, oil and energy infrastructure and facilities, military and police facilities, and personnel, abductions, and attacks against former FARC leadership have become the primary focus of terrorist attacks in Colombia.[10]

Biological or Other Weapons of Mass Destruction

During the Colombian conflict, several extremely low-grade incidents occurred that can be loosely classed as bioterrorism. These incidents involved the contamination of bullets with various biological substances, including human excrement.[11] But neither the Revolutionary Armed Forces of Colombia nor the National Liberation Army appear to have possessed any interest in pursuing weapons of mass destruction (WMDs), despite the groups' pursuit of advanced conventional capabilities.

Chile

Chile has seen a rise in left-wing terrorism and indigenous insurgency since 2010.[12] Although the number of violent incidents has increased over time, thus far, they have not resulted in significant numbers of injuries or deaths. Aside from a few noteworthy exceptions, the consequences of these attacks have mostly been property damage. Nothing has indicated any of the groups engaged in ideologically motivated violence in Chile have developed, or are likely to develop, any interest in the use of biological materials.

Terrorist/Insurgent Groups

Foreign

The Lebanon-based Hezbollah purportedly maintains a limited presence in Chile—primarily, in the form of various front companies operating in the Zona Franca de Iquique.[13] Hezbollah has also been alleged to be connected to transnational criminal organizations and the smuggling of illicit substances via Chile.[14] Available information indicates Chile primarily serves as an economic resource for Hezbollah, though the group may use personnel and facilities in the country for logistical support or operational coordination for Hezbollah's activities throughout South America. Much open-source material on Hezbollah's activities in Chile repeats older information related to the group's activities in the 1990s and early 2000s; thus, determining how much of this information remains valid in the 2020s is difficult.

Domestic

Domestic terrorism and insurgency have been a problem for the Chilean government for several decades, and this trend appears to have been growing in significance since 2010.[15] Two primary ideological sources of conflict have fueled the ongoing attacks.

The first is left-wing extremism, typically of an anticapitalist or anarchist nature. Chile has a long tradition of left-wing terrorism, which was particularly strong during the period of military rule from 1973–90. Thereafter, the violence declined significantly. The left-wing violence began to increase once more starting in 2007. Nevertheless, at no point has the violence approached the levels seen in the 1980s.[16] The left-wing groups mounting attacks use multiple names. But whether the identified groups represent the only perpetrators of violence and whether all named groups represent distinct groups are unclear. As such, additional independent, left-wing actors—either individuals or small cells—may be contributing to the attacks.

The second source of extremism in Chile is an indigenous movement that consists of multiple groups and focuses on opposing the Chilean state in the Mapuche conflict.[17] Goals of the movement include the protection of indigenous rights; the return of land taken from the indigenous people in the nineteenth and twentieth centuries; and, potentially, the independence—or at least, regional autonomy—of the Región de la Araucanía, located between Chile and Argentina.[18] The intensity of the dispute between the Mapuche community and the Chilean government hasintensified since 2015, with increasing numbers of armed clashes between Chilean government personnel and Mapuche extremists.[19] The frequency of arson attacks and other sabotage directed at logging companies operating in the Región de la Araucanía and Los Ríos Region has continued to increase as recently as 2022.[20] Table 5-3 provides a list of Chile's currently active domestic terrorist and insurgent groups.[21] In this context, biosecurity relevance is based on whether the group has undertaken attacks against biosecurity infrastructure or has demonstrated interest in the pursuit or use of biological agents as weapons. In addition, the incident column records the year of the most recent incident recorded in the National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database for the group.

Table 5-3. Active domestic terror or insurgent groups in Chile

Group	Activity	Incident	Still Active?	Biosecurity Relevance
Antagonistic Nuclei of the New Urban Guerrilla	Terrorism	2016	Yes	No
Arauco-Malleco Coordinating Group – Chile	Terrorism	2020	Yes	No
Cómplices Sediciosos/Fracción por la Venganza		2019	Unknown	No
Individuals Tending toward Savagery		2019	Unknown	Yes
International Revolutionary Front		2016	Unknown	No
Lautaro Youth Movement		2018	Unknown	No
Weichán Auka Mapu	Terrorism	2020	Yes	No

The Arauco-Malleco Coordinating Group has existed since 1998. The Spanish name for Individuals Tending toward Savagery is Individualistas Tendiendo a lo Salvaje. If this group still operates, it could potentially pose an external threat to chemical and biological facilities and laboratories, given Individuals Tending toward Savagery's tendency to target scientific institutes and companies that deal with nanotechnology. The group does not appear to have any interest in using or acquiring a biological agent as a weapon.

Terrorist/Insurgent Incidents since 2010

Conventional

Since 2010, Chile has seen extensive extremist violence that has involved the use of small IEDs or arson. Since 2018, terrorist attacks have predominantly targeted forestry equipment (for example, trucks and backhoes), facilities, and companies.[22]

Bombings by left-wing extremists, representing an unknown number of genuine groups, continue. Although most incidents have appeared to prioritize property damage over taking lives, this trend has not always been the case. In addition to economic targets, such as foreign business interests, attacks are frequently directed at police stations or gendarmerie facilities.[23] In September 2014, a particularly serious event resulted in the injury of 14 people when a bomb placed in a subway trash can exploded.[24] In February 2020, several incendiary devices were thrown into a church where approximately 150 people were meeting to discuss the upcoming April 2020 constitutional referendum.[25]

Multiple violent incidents between police and extremists have occurred in the Mapuche conflict. As noted above, the frequency and severity of incidents such as arson attacks and armed confrontations have been increasing over time, with little indication that the attacks will end in the near-to-medium term.[26]

Biological or Other Weapons of Mass Destruction

Nothing has indicated any Chilean extremist groups have explored or attempted the use of biological warfare agents or any other form of biological attack. The pursuit and use of biological agents or other WMDs would represent a significant departure from the typical pattern of activity associated with the Chilean domestic extremists. Finally, no foreign extremist groups associated with the use of biological agents or other WMDs are currently known to be active in Chile.

Biosecurity Specific Legal Frameworks

Colombia

Colombia possesses a critical core of biosecurity-related legislation and regulation that provide a breadth of application. But in comparison, this critical foundation of biological and biosecurity legal framework (legislation and regulation) is much smaller than the expansive legislation and regulation formulated to combat nuclear and radiological material proliferation.

International Law Relevant to Biosecurity

Treaties, Conventions, and Agreements

Colombia is a member of two key conventions and protocols relevant to biosecurity: the Biological Weapons Convention (BWC) and the Geneva Gas Protocol. As an active member state party to the BWC, Colombia continues to submit annual Confidence Building Measures

(CBM) reports and has done so since 2014.[27] The earliest record of Colombia submitting a CBM report is from 1998. Colombia did not submit another CBM report until 2012. Although CBM report submissions by member state parties are inaccessible to the public, the Resolution 1540 Committee provides a yearly submission record that shows Colombia's long-time engagement with submitting CBMs (since 1998) and sustaining yearly submissions (since 2014).[28]

Colombia also engages with regional partners and international organizations for voluntary assistance and training. Examples of such engagement include the country's 2019 work with the BWC Implementation Support Unit and the Organization of American States in various BWC-support and related workshops.[29] Colombia has also partnered with Chile in recent years, which "led to development of a laboratory survey and to improved processes for collecting information from agencies."[30] Security Council Resolution 1540 is a crucial resolution that extends to all countries, and through efforts to support this resolution, Colombia continues to partner with the council's Resolution 1540 Committee to improve the country's training, enacted legislation, and technical capabilities and capacities.[31] Throughout this engagement, Colombia has enacted an extensive set of laws and regulations to prevent non-state actors from engaging with, acquiring, and developing chemical, nuclear, or biological agents or materials.

Organizations

Colombia is an active member of several international organizations that work in the biosecurity space, including the World Health Organization and its subsidiary, the Pan American Health Organization; the World Organisation for Animal Health (founded as the Office International des Espizooties); the Organization of American States; the International Maritime Organization; the International Criminal Police Organization; and the World Customs Organization—specifically, its *SAFE Framework of Standards* and the Proliferation Security Initiative.

Domestic Legislation and Regulation

Colombia has an extensive history of legislation and regulation that covers several aspects of biosecurity, including national basic requirements for the country's National Network of Laboratories for biosafety and biosecurity protocols and procedures; import, export, and transport controls on biological materials; and disease surveillance and bioethics for research. Among this extensive legal framework is legislation to address money laundering and combat terrorism and threats emanating from non-state actors.

Colombia has several regulations and laws in place that specifically address biosecurity issues at the national level, such as regulations governing all public health laboratories, bioethical standards in research, and controls for handling, researching, transporting, and producing living modified organisms. (The term "living modified organisms" is specifically employed in the Convention on Biological Diversity.) Although these regulations and laws typically frame these issues around biosafety, the regulations and laws constitute a critical foundation upon which the Colombian state can address biosecurity issues as well. Several examples include the following:

- Resolution no. 2935 (October 23, 2001) – Established research guidelines for genetically modified organism biosafety as well as research information security.
- Resolution no. 3832 (1997) – Covers the cross-border transport of biological materials.
- Lineamientos Generales de Bioseguridad y Biocontención para los laboratorios de la Red Nacional de Laboratorios (2020) – Provides guidance for the National Network of Laboratories on biosafety and biosecurity protocols.
- Decree no. 2323 (2006) – Created the structure of the National Network of Laboratories and a mechanism for monitoring activities.
- Decree no. 3518 (2006) – Created and established regulations for the Surveillance System on Public Health.
- Resolution no. 1619 (2015) – Established a review process for the submission and evaluation of laboratory self-assessments and reports.
- Law no. 489 (1998) – Assigned oversight, adherence, and compliance responsibilities and authorities to ministries and administrative departments.
- Law no. 1955 (2019) – Oversees regulations on and access requests for biological collections and genetic resources (Ministry of Environment and Sustainable Development).

Finally, Colombia possesses a solid, though small, base of legal frameworks that combat proliferation, including several regulations that control the importation, exportation, and transportation of biological materials as well as munitions.

Chile

Chile works extensively with international organizations on matters of biosecurity. The country is a member of several key international treaties, conventions, and agreements that lie at the heart of global biosecurity efforts.[32] Chile also works extensively with the UN Office of Disarmament Affairs on key WMD nonproliferation issues as well as the Security Council's 1540 Committee to prevent the use of, acquisition of, access to, and proliferation of WMD materials, including biological agents and related materials, by non-state actors. Much of Chile's domestic legal framework, therefore, supports nonproliferation, whether the legislation addresses the financing of terrorism, illicit trade, or the security of trade and maritime control. This focus is also important given that Chile is a key regional exporter of raw materials and agricultural products.

International Law Relevant to Biosecurity

Treaties, Conventions, and Agreements

Like Colombia, Chile is a member of two key conventions and protocols relevant to biosecurity: the BWC and the Geneva Gas Protocol. As an active member state party to the BWC, Chile continues to partner with numerous and diverse member states to propose, cosponsor, and submit multilateral proposals and training activities to support the advancement and fulfillment of the BWC.[33] Chile also provides regular annual CBM reports.[34] To support Security Council Resolution 1540, Chile has also enacted an extensive set of laws and regulations to prevent non-state actors from engaging with, acquiring, or developing chemical, nuclear, or biological agents or materials.

Organizations

Chile is an active member of several international organizations that work in the biosecurity space, including the World Health Organization and its subsidiary, the Pan American Health Organization; the World Organisation for Animal Health; and the Organization of American States. Additionally, Chile has long-term ties with the Proliferation Security Initiative, which supports existing international nonproliferation resolutions, treaties, and multilateral regimes in preempting interdictions of illicit WMD materials.

Domestic Legislation and Regulation

Chile appears to have one prevailing biosecurity regulation, entitled *Manual de normas de bioseguridad y riesgos asociados* (Manual on Norms of Biosecurity and Related Risks), published by the National Commission for Scientific and Technological Research.[35] Much of this particular regulation also includes biosafety standards. But chapter nine of the regulation speaks directly to the biosecurity concerns of intentional release or the exposure of biological materials.[36] This regulation also presents a breadth of requirements for laboratories and biological research centers, the training that is expected, equipment, facility design, and leadership responsibilities.

Finally, Chile has established a lengthy list of regulations, laws, decrees, and so forth that provide avenues of response to biological material proliferation issues—namely, through customs, import, transport, and health sanitary codes.

Biosecurity Threat Assessment of Colombia and Chile

Colombia

Terrorist and insurgent groups in Colombia today are mostly domestic actors that neither extend nor present a possible venture into any use of biological agents—rather, the groups stay with conventional forms and weapon types. Dissident domestic groups of the Revolutionary Armed Forces of Colombia as well as the National Liberation Army continue to occupy the Colombian government's attention as the primary terrorist and insurgent groups. These groups, which also apply pressure to the 2016 Peace Accords, are the main security concern within the country. As such, the threat of conventional terrorism and insurgency in Colombia remains elevated. But the threat of bioterrorism remains low for the near term to the midterm.

Colombia possesses a critical core of biosecurity-related laws and regulations that provide a breadth of application. This core of national legislation on biosecurity-related matters provides Colombia with a broad capacity to continue to expand the country's health, biosecurity, and nonproliferation response activities. Critical focus is provided to monitor imports and exports, allow controls and regulations for appropriate licensure, and increase the level of compliance and implementation for national and international regulations in the vast National Network of Laboratories at the national and local levels.

Expanded regulations to increase disease monitoring of imported animals and animal products to prevent invasive, introduced biological, or other materials from entering the country as well as expanded regulations to increase disease monitoring within domestic livestock to ensure export viability are areas where the expansion of regulations would provide significant added capability to Colombia's biosecurity posture.

Finally, the current overall biosecurity threat for Colombia is assessed to be low. This assessment is driven by a lack of active terrorist or insurgent threats as well as a robust regulatory structure and active government engagement in biosecurity.

Chile

Terrorism in Chile is primarily a domestic phenomenon. No operational or ideological indicators suggest any domestic terrorist or insurgent groups currently operating on Chilean soil have developed, or are likely to develop in the near- to medium-term, any interest in the acquisition or deployment of biological agents. Domestic left-wing extremists pose a small biological risk because their targeting of foreign businesses introduces the possibility that research facilities that handle biological materials may be targeted, potentially causing an inadvertent or unintentional release in addition to the direct risk to the safety of personnel. Accordingly, the overall risk of terrorist or insurgent engagement with biological agents in Chile is assessed to be low, with the sole exception noted above.

Chile's regulatory landscape provides a solid foundation that covers the breadth of biosecurity concerns at the national level, including the implementation and authorization of the BWC, safety and security at ports, the safe handling of biological materials during transport, national biosecurity standards, and guidance for clinical laboratories (including personnel, protective equipment, and intentional and accidental release response).

Finally, the current, overall biosecurity threat for Chile is also assessed to be low, owing to the country's robust regulatory structure and active government engagement in biosecurity, coupled with a lack of active indications terrorist or insurgent groups are pursuing biological agents within Chilean borders.

Conclusion: Emerging Threats and Recommendations for NATO

Although the biosecurity threat levels for Colombia and Chile are currently low, both countries must consider the potential for emerging biosecurity threats over the next five to 10 years. Colombia and Chile have growing biomedical and biotechnology research and production industries as well as active government programs designed to encourage continued growth and international partnerships in the industry. With this backdrop, the implication is that as the two countries' biomedical and biotechnology capacities grow, so will the countries' biosecurity attack surfaces that are vulnerable to nefarious threat actors. Studies have shown terrorists and criminals primarily follow the path of least resistance—that is, if you challenge them in one location, they will shift to another location where they are not as challenged.[37] Likewise, because increased biosecurity vulnerabilities have accompanied the increase in biomedical and biotechnology capacities, Colombia and Chile will become attractive destinations for those seeking to acquire biological agents or materials for nefarious purposes—at least, until Colombia and Chile can develop and implement appropriate policies and measures to address these newfound vulnerabilities. From this perspective, Colombia and Chile must be prepared for the emerging threat emanating from VNSAs from within and outside the countries' borders as Colombia's and Chile's biomedical and biotechnology capacities increase over time.

Recommendations for NATO

As an organization or as individual member states, NATO could engage in several activities to ensure Colombia and Chile can successfully mitigate emerging biosecurity threats as they continue to build their biomedical and biotechnology capacities. These activities include the following.

- Share best practices for building a biosecurity culture and raise awareness among Colombia's and Chile's biotechnology industries and government personnel as well as the the general publics on the potential threat that accompanies increased biomedical and biotechnology capacities, paying specific attention to:

  - the protection of technology;
  - research ethics;
  - business ethics;
  - wealth distribution; and
  - the navigation of social issues that stem from new technologies or evolving political, social, or economic structures (that can be attributed to the advancement and growth of the biotechnology industry).

- Share best practices for developing and implementing national policies, laws, and regulations that meet the development goals of the countries, have the regulatory and enforcement mechanisms necessary to mitigate potential emerging threats, and are socially responsible and just.
- Conduct joint training exercises—both military and intergovernmental—to increase response capabilities in case of natural, accidental, or deliberate biological events.
- Share emerging threat information to ensure Colombia and Chile are in the best position to respond as necessary.

Endnotes

1. Esteban Ortiz-Prado et al., "Vaccine Market and Production Capabilities in the Americas," *Tropical Diseases, Travel Medicine and Vaccines* 7 (April 2021): https://doi.org/10.1186/s40794-021-00135-5.

2. Kreativ Information AB, "Colombia Bets on Vaccine Production," Kreab Worldwide (website), January 4, 2022, https://kreab.com/bogota/en/insight/colombia-bets-on-vaccine-production/; "Construction Begins on VaxThera Plant to Produce Vaccines and Biologicals for Colombia and the Rest of the Region," Grupo SURA (website), February 18, 2022, https://www.gruposura.com/en/noticia/construction-begins-on-vaxthera-plant-to-produce-vaccines-and-biologicals-for-colombia-and-the-rest-of-the-region/; "VaxThera, Seguros SURA Colombia's New Biotechnological Investment, Seals an Alliance for Strengthening Vaccine Development Both in Colombia and the Rest of Latin America," Grupo SURA (website), June 13, 2022, https://www.gruposura.com/en/noticia/vaxthera-seguros-sura-colombias-new-biotechnological-investment-seals-an-alliance-for-strengthening-vaccine-development-both-in-colombia-and-the-rest-of-latin-america/; Silvia Gutierrez, "Colombia: Biotech Business Opportunities," Switzerland Global Enterprise (website), June 1, 2023, https://www.s-ge.com/en/article/global-opportunities/20183-c6-life-science-opportunities-colombia?ct; Christin Boldt, "Chile," Bioökonomie.De (website), May 7, 2022, https://biooekonomie.de/en/topics/in-depth-reports-worldwide/chile; and Foreign Agricultural Service, *Agricultural Biotechnology Annual: Colombia*, Report no. CO2022-0018 (Washington, DC: Department of Agriculture, 2022).

3. Julian Hitchcock, "DIY Gene-Editing CRISPR Kits," Bristows (website), January 6, 2021, https://www.bristows.com/news/diy-gene-editing-crispr-kits/; Paul Kumst, "CRISPR—A Rogue One?," *Georgetown Security Studies Review* (blog), November 8, 2016, https://georgetownsecuritystudiesreview.org/2016/11/08/crispr-a-rogue-one/; Lana Schwartz, "I Edited Human DNA at Home with a DIY CRISPR Kit," *Vice* (website), January 26, 2023, https://www.vice.com/en/article/qjkykx/diy-crispr-gene-editing-kit-human-dna; and Annie Sneed, "Mail-Order CRISPR Kits Allow Absolutely Anyone to Hack DNA," *Scientific American* (website), November 13, 2017, https://www.scientificamerican.com/article/mail-order-crispr-kits-allow-absolutely-anyone-to-hack-dna/.

4. Steve S. Sin and Markus K. Binder, "Violent Non-State Actor CBRN Event Database," Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism Asymmetric Threats Analysis Center (website), last updated December 8, 2022, https://cbrn.umd.edu/event_database.

5. Darryl Heeralal, "Terror Threat: Islamic Group Unveils Secret 'Chemical Labs,' " *Trinidad Express*, January 26, 2003; Caribbean Media Corporation, "Trinidad and Tobago to Overhaul Anti-Terrorism Laws," *BBC Summary of World Broadcasts*, February 13, 2003; Agência Estado, "US Consulate Employee in Brazil Ill After Opening Envelope Containing Powder," trans. BBC Monitoring, *BBC Summary of World Broadcasts*, September 12, 2003; "US Consulate General in Brazil Receives Envelope Containing Suspicious Powder," *Folha de Sao Paulo*, September 13, 2003; "Colombian Army Says FARC Rebels Using Cyanide-Tipped Bullets," *El Espectador*, August 10, 2005; "EPL Used Cyanide-Tipped Bullets," *El Colombiano*, August 15, 2005; and "EPL Claims Killing of 4 Police Officers in Norte de Santander," *El Tiempo*, August 15, 2005.

6. Bureau of Counterterrorism, "Country Reports on Terrorism 2020: Colombia," Department of State (website), December 16, 2021, https://www.state.gov/reports/country-reports-on-terrorism-2020/colombia__trashed/.

7. Bureau of Counterterrorism, "Foreign Terrorist Organizations," Department of State (website), July 6, 2023, https://www.state.gov/foreign-terrorist-organizations/.

8. Bureau of Counterterrorism, "Foreign Terrorist Organizations."

9. Juan Diego Posada, "Implicaciones del regreso a la guerra de los líderes de las FARC," InSight Crime (website), February 4, 2021, https://es.insightcrime.org/noticias/analisis/implicaciones-del-regreso-a-la-guerra-de-los-lideres-de-las-farc/; and Luis Jaime Acosta, Julia Symmes Cobb, and Jonathan Oatis, "Colombia Military Kills FARC Dissident Leader Mordisco," Reuters (website), July 15, 2022, https://www.reuters.com/world/americas/colombia-military-kills-farc-dissident-leader-mordisco-2022-07-15/.

10. "Global Terrorism Database," National Consortium for the Study of Terrorism and Responses to Terrorism (website), last updated May 2022, https://www.start.umd.edu/gtd.

11. "EPL Claims Killing of 4 Police Officers in Norte de Santander," *El Tiempo*, August 15, 2005.

12. "Chile: Extremism and Terrorism," Counter Extremism Project (website), n.d., accessed on November 10, 2023, https://www.counterextremism.com/countries/chile-extremism-and-terrorism; and "Global Terrorism Database."

13. Alma Keshavarz, "Iran and Hezbollah in the Tri-Border Areas of Latin America: A Look at the 'Old TBA' and the 'New TBA,'" *Small Wars Journal* (blog), November 12, 2015, https://smallwarsjournal.com/jrnl/art/iran-and-hezbollah-in-the-tri-border-areas-of-latin-america-a-look-at-the-%E2%80%9Cold-tba%E2%80%9D-and-the.

14. Bureau of Counterterrorism, *Country Reports on Terrorism 2021* (Washington, DC: Department of State, 2021), 191.

15. Counter Extremism Project, "Chile: Extremism and Terrorism"; and "Global Terrorism Database."

16. "Global Terrorism Database."

17. Jack Herscowitz, "The Mapuche-Chilean Land Conflict and Justice: Re-Contextualizing 21st Century Violence," *Towson University Journal of International Affairs* 52, no. 2 (Spring 2019): 14–33, https://wp.towson.edu/iajournal/mapuche-page-draft/.

18. Herscowitz, "Mapuche-Chilean Land Conflict."

19. Counter Extremism Project, "Chile: Extremism and Terrorism"; and Lucia Newman, "A Journey through Chile's Conflict with Mapuche Rebel Groups," *Al Jazeera* (website), April 12, 2021, https://www.aljazeera.com/features/2021/4/12/a-journey-through-chiles-conflict-with-mapuche-resistance-groups.

20. Paola Camero, "Ataque incendiario en Mariquina: fiscalía apunta motivación en la causa Mapuche y la libertad de algunos presos," *Soy Chile* (website), February 15, 2022, https://www.soychile.cl/valdivia/sociedad/2022/02/15/744611/encapuchados-queman-18-camiones.html.

21. Paulo Muñoz Alarcón, "Fiscalía sur indagará si artefacto en vitacura corresponde a reivindicación en caso bombas," *La Tercera* (website), February 17, 2020, https://www.latercera.com/noticia/fiscalia-sur-indagara-si-artefacto-en-vitacura-corresponde-a-reivindicacion-en-caso-bombas/; El Mostrador/EFE, "Web anarquista publica comunicado de grupo que se adjudicó el envío de los paquetes bomba a la comisaría y Hinzpeter," *El Mostrador* (website), April 7, 2023, https://www.elmostrador.cl/noticias/pais/2019/07/29/web-anarquista-publica-comunicado-de-grupo-que-se-adjudico-el-envio-de-los-paquetes-bomba-a-la-comisaria-y-hinzpeter/; and "Weichan Auka Mapu: Los descolgados radicales de la CAM," *Soy Chile* (website), September 3, 2017, https://www.soychile.cl/Temuco/Policial/2017/09/03/485258/.

22. "Global Terrorism Database."

23. GardaWorld, "Chile: Explosives Attack Dec. 27 in Santiago Causes No Casualities," *Crisis24* (blog), December 27, 2021, https://crisis24.garda.com/alerts/2021/12/chile-explosives-attack-dec-27-in-santiago-causes-no-casualities.

24. "Global Terrorism Database."

25. "Molotov Bomb Thrown into Congregation in Chile," Lutheran World Federation (website), March 10, 2020, https://www.lutheranworld.org/news/molotov-bomb-thrown-congregation-chile.

26. Camero, "Ataque incendiario en Mariquina"; and Newman, "Mapuche Rebel Groups."

27. Security Council Committee Established Pursuant to Resolution 1540 (2004), *Approved 1540 Committee Matrix (Republic of Colombia)* (New York: UN, 2020).

28. Security Council Committee Established Pursuant to Resolution 1540 (2004), *Approved 1540 Committee Matrix*.

29. Richard Guthrie, *2019 Meeting of States Parties: Setting the Scene (Tuesday 3 December)*, Meeting of States Parties (MSP) Report no. 1 (Geneva: BioWeapons Prevention Project [BWPP], 2019); Richard Guthrie, *The Opening of the 2019 BWC Meeting of States Parties (Wednesday 4 December)*, MSP Report no. 2 (Geneva: BWPP, 2019); Richard Guthrie, *The General Debate Ends and Discussion of the Meetings of Experts Begins (Thursday 5 December)*, MSP Report no. 3 (Geneva: BWPP, 2019); Richard Guthrie, *Three MXs, Preparations for the Review Conference and Annual Reports (Friday 6 December)*, MSP Report no. 4 (Geneva: BWPP, 2019); and Regional Centre for Peace, Disarmament and Development in Latin America and the Caribbean, "UNLIREC and VERTIC Assist the Government of Colombia in Implementation of Biological and Toxin Weapons Convention," news release, November 3, 2021, https://unlirec.org/en/unlirec-and-vertic-assist-the-government-of-colombia-in-implementation-of-biological-and-toxin-weapons-convention.

30. UN Office of Disarmament Affairs, *Report on BWC Relevant Developments by International Experts – Submitted by Malaysia and the United States of America*, Report no. BWC/MSP/2017/WP.24 (New York: UN, 2017).

31. Security Council Committee Established Pursuant to Resolution 1540 (2004), *Approved 1540 Committee Matrix*.

32. UN Institute for Disarmament Research, "Chile," Biological Weapons Convention National Implementation Measures Database (website), 2023, https://bwcimplementation.org/states/chile.

33. Parliamentarians for Global Action, "Regional Parliamentary Workshop to Promote Ratification and Implementation of the Biological and Toxin Weapons Convention (Santiago, Chile)," press release, May 29, 2017, https://www.pgaction.org/news/regional-parliamentary-workshop-santiago.html.

34. Biological Weapons Convention Implementation Support Unit, "Chile," Biological Weapons Convention Electronic Confidence Building Measures Portal (website), n.d., accessed on November 6, 2023, https://bwc-ecbm.unog.ch/state/chile.

35. Fondo Nacional de Desarrollo Científico y Technológico, *Manual de normas bioseguridad y riesgos asociados* [Manual on norms of biosecurity and related risks] (Santiago, CL: Comisión Nacional de Investigación Científica y Technológica, 2018).

36. Fondo Nacional de Desarrollo Científico y Technológico, *Norms of biosecurity*, 170–76.

37. Frank O. Mora, "Victims of the Balloon Effect: Drug Trafficking and US Policy in Brazil and the Southern Cone of Latin America," *Journal of Social, Political, and Economic Studies* 21, no. 2 (1996): 115.

– 6 –

Nanoweaponry and the Resolution Revolution: Making Danger Invisible

Darrin L. Frye

> "In the past century, scientists began to leave their comfort zone to voyage into the micro world, the molecular world unseen to us. Now, the time has come for us to be pilgrims of the nanoworld, to colonize the micro. This colonization will be propagated by the nanotechnological revolution."[1]

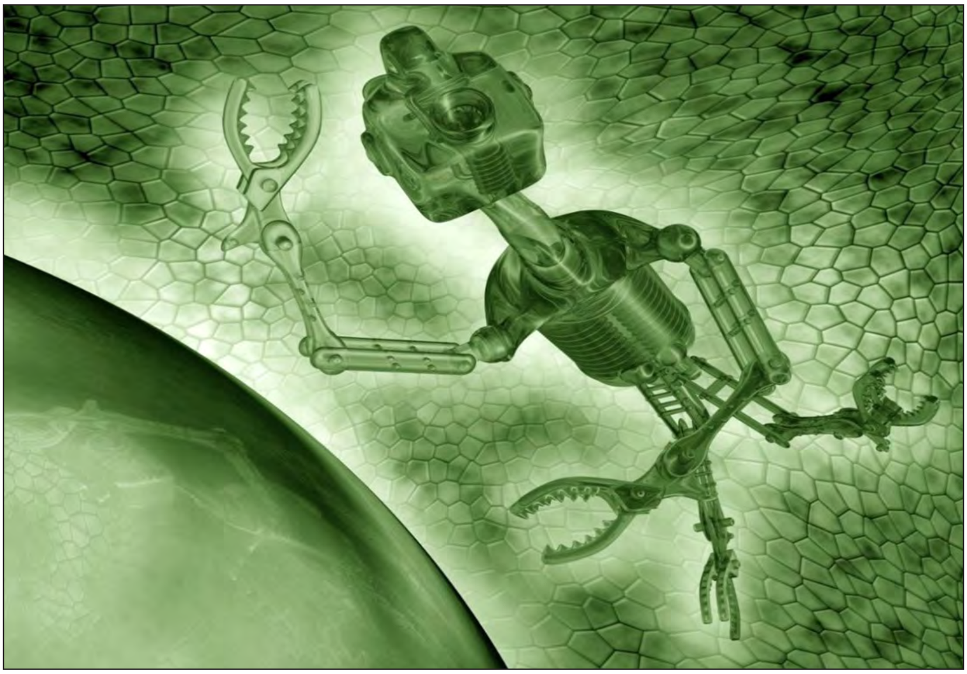


Figure 6-1. Artist's rendering of a nanobot
Image used through author's purchase of license from Stock Photos by Dreamstime.

Introduction

Humankind relentlessly probes the expanse of our universe and plunges to the depths of the oceans, perpetually driven by an insatiable quest for answers about our origins and existence. Innovators have gifted adventurers with advanced tools, granting humankind the extraordinary ability to see, hear, conceptualize, and experience exploration like never before.

In 1931, Dr. Ernst Ruska invented the electron microscope, which was foundational to advancing nanoscience.[2] Ruska's achievement provided a window through which to see past the invisible for the first time. Ruska's magical microscope triggered a vast resolution revolution, spurring bold scientific pilgrims to try to colonize the unknown, microcosmic frontier of nanoscience.[3] As our fascinations stretch outward past the clouds or deep below the waves, many investigations are now directed inward. In this new super-resolution revolution, we see an "impressive proliferation of new instruments for imaging at higher resolution, imaging single molecules and faster and more sensitive multidimensional live cell imaging."[4] Now, explorers are refocusing their lenses, embarking on incredible microscopic odysseys, and hoping to unravel the complexities of the magical microuniverse. Researchers are discovering unique quantum properties as the researchers enter the minuscule nanoscale world, and they are busily incorporating their incredible findings into novel tools to enable, enrich, and empower our society.

The study of ultrasmall nanotechnology has ushered in a new, magnified era of scientific development that encourages innovative thinkers to adjust their perspectives and create groundbreaking technologies at an unprecedented pace. In 2012, notable scientists Dr. Emmanuelle Charpentier and Dr. Jennifer Doudna invented a revolutionary method of editing the deoxyribonucleic acid (DNA) code, selectively called "clustered regularly interspaced short palindromic repeat."[5] This invention significantly accelerated genomic scientists and innovators' development of new research goals, such as characterizing the DNA code and curing all genetic diseases. But alongside this fantastic progress and the numerous positive contributions nanoscience makes to society, those with malicious intentions are increasingly developing tools of destruction.[6] Across the world, microweaponry designers and nefarious actors are busily manipulating nanomolecular properties to craft tiny yet highly destructive instruments of terror that pose grave threats to humanity.[7]

These minuscule weaponry creators use newly discovered, molecular-scale properties to design technologies that evade detection and increase stealth.[8] Newly minted munitions present significant risks because the nanotechnologies' size, low cost, scalability, and unmatched targeting precision make them innately suitable for covert activities. "Super terrorists" with access to nanoweaponry will have the opportunity to threaten entities that have enjoyed relative immunity to traditional modes and past methods of terrorism.

Nanoweapons and the New Battlefield

Both the size of the weaponry and the sites of future battles have shifted. Typically, targets of terror are two-meter-tall people, but in the future, minuscule robotic weapons will aim at targets that are two nanometers high—a billion times smaller. This shift toward miniaturized targets is disruptive and drastically alters how terrorism, competition, and conflict will be conducted. Just a handful of nanosoldiering robots could seize control of an entire nation temporarily or permanently. Astonishingly, more than three billion nanosoldiering robots could fit within a teaspoon.[9]

Nanotechnology—manipulating matter on a molecular scale—holds immense potential for transformative achievements across various fields. But with nanotechnology's great promise comes the lurking danger of nanoweaponry—a new realm of precision threats that are virtually invisible and capable of causing catastrophic harm. This chapter will discuss psychological and physical injuries, the nearly impossible mitigation processes involved in stopping nanoweaponry, and nanoweaponry's compounding impact on existing threats. A logical forecast is one in which protecting life, DNA, and the environment becomes paramount, underscoring the urgent need for global cooperation to navigate the treacherous waters of accessible and generational nanoweaponry.

Consequently, evaluating the weaponization of nanotechnology; discussing the diminutive size of new, intracellular combatants and invisible, minuscule battlefields; and recognizing the physical, mental, and programmable risks posed by each of these new threats is essential. We must alert and inform leaders, decisionmakers, and all those governed by them to prevent life on this planet from being turned into a soupy "grey goo" by enemies of humanity who might choose to use one of these immensely powerful munitions.[10]

Increased Peril of Invisibility

Understanding the world of nanotechnology requires grappling with the concept of the nanoscale, a realm too small to be visible to the naked eye.[11] Although many developmental pathways exist for nanotechnology and its weaponization, one of the lesser-discussed pathways is how nanomunitions can target human cells, producing horrors beyond imagination. Now, nations must prepare for intranuclear threats from the emerging genomic war, with mitigation plans distinctly different from those of the Cold War. This new battle is different from past battles, when "nuclear threat" meant something entirely different. In the past, we practiced "duck and cover" drills in school, as depicted in figure 6-2, in response to the fear of nuclear weapons dropping from overhead.[12] Now, we must work against the possibility of microexplosions from deep within, where hiding or sheltering is impossible.

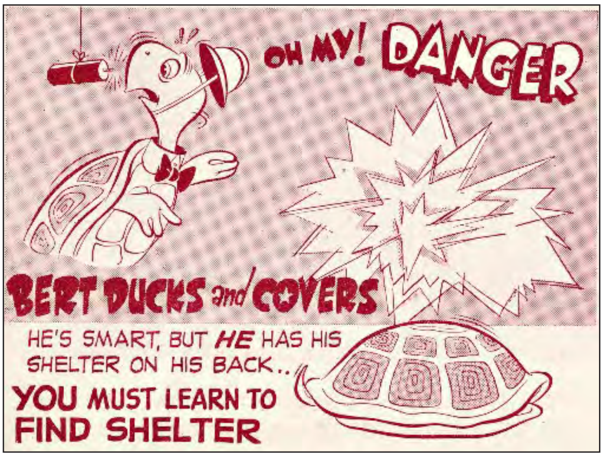

OH MY! DANGER
BERT DUCKS and COVERS
HE'S SMART, BUT HE HAS HIS SHELTER ON HIS BACK..
YOU MUST LEARN TO FIND SHELTER

Figure 6-2. A page from a pamphlet produced by the Federal Civil Defense Administration in 1951

In the tiny nucleus of every cell, DNA, the double-stranded molecule carrying life's building blocks, is a crucial target for nanoweapons. The human cell is about 10,000 nanometers in diameter; the nucleus, 5,000 nanometers; ribosomes, 25 nanometers; and DNA, 2.5 nanometers. Because all bodily functions rely on accurate reading and replication of the code DNA contains, any weaponized errors inserted into this precious template will be catastrophic. The ribosomes, a nuclear neighbor, take the information copied from DNA and manufacture essential products that allow bodily systems to function. Weapons could create lethal conditions by feeding ribosomes corrupted information or damaging them to the point at which they are inoperable. At this scale, nanoweapons a few nanometers in size can easily infiltrate living organisms through inhalation, ingestion, absorption, or even reproduction. These intruders can bypass all human defense mechanisms to attack vital brain and body cells with impunity.

Due to their tiny size, nanorobotic vectors can operate without any discernible movement, sound, or motion to give away their presence. The only indication of nanorobotic vectors' arrival would be the trail of destruction and chaos left behind. These nanoweapons present a threat that could emerge from any direction, at any moment, without warning, truly making danger invisible.

Due to their mechanisms of action, nanoweapons offer an exceptional level of programmability. A nanorobot could adhere to a DNA target at any of the 3.2 billion base locations along the target's structure and wait to disrupt the thousands of genes that produce the substances required for life.[13] These disruptors could target energy production, growth, reproduction, or critical chemical processes. Because every human has a unique genetic code, a single person could be targeted and efficiently sorted out from billions of others if his or her genetic code were known. This capability would empower terrorists and other adversaries to tune their effects proficiently. Recognizing these dangers underscores the urgency of implementing proactive strategies to mitigate the havoc belligerents could wreak for all living things using nanoweapons.

The advanced targeting and precision capabilities of nanomunitions grant malicious actors the ability to stretch their resources. Because intentionally targeting civilians and producing visible carnage are hallmarks of terrorism, terrorists might use nanomunitions in other ways—namely, to evoke fear rather than direct damage. Many believe fear is the most destructive weapon. Jenny Holzer captured this point of view in her work *Untitled (Fear Is the Most Elegant Weapon . . .), from Inflammatory Essays*: "Fear is the most elegant weapon, your hands are never messy. Threatening bodily harm is crude. Work instead on minds and beliefs, play insecurities like a piano. Be creative in approach. Force anxiety to excruciating levels or gently undermine public confidence.

Panic drives human herds over cliffs; an alternative is terror-induced immobilization. Fear feeds on fear."[14] Although the ideas behind Holzer's work are frightening, it supports the notion that emotional injuries usually outlast physical ones.

Nanomunitions could target specific populations, including certain age groups, genders, ethnicities, or classifications. Because of their diminutive size, nanoweapons can be amassed in massive quantities while remaining compact and dispersed through various media, such as air, water, and food. Immediate consequences from exposure are possible, but easily disseminated nanoweapons can remain dormant, activate slowly, and become impossible to prevent or treat once introduced.

Targeting Brain Functions

The ability to threaten brain functions with nanoweapons adds a sinister dimension to nanoweapons' possible damage. Manipulating cognitive and neural processes with invisible munitions could lead to a spectrum of outcomes, from impaired decision making to distorted perceptions of reality. Disruptions to the neurological system could extend to sensory systems, creating blindness, hearing loss, alterations in smell and taste, searing pain, and other maladies. This permeable brain threat could also impact performance, creating conditions that affect coordination, balance, speed, strength, and stamina. Although living systems have the security to prevent and protect themselves from intrusion, these elusive munitions bypass standard barriers to entry.

Nanobots can effortlessly breach the human blood-brain barrier, a powerful safeguarding mechanism designed to shield our most valuable assets: the brain and spinal cord.[15] This barrier maintains sterility and typically filters out infectious intruders, relegating them to the peripheral body system, where local defenses can isolate and eliminate them quickly. Although affected hosts might recognize nanobots as foreign, they could disconnect the emergency notification system, literally turning off the alarm. Additionally, nanobots could execute damages to critical bodily functions long before the overwhelmed immune-response process can be successfully generated, assuming it has not already been compromised.

Innumerous physical wounds have occurred in global combat, and all types have been well documented since 2000 BC.[16] But with nanoweaponry, a new menace emerges, with potential damages transcending physical health and corrupting mental health. Intentional emotional sabotage could cause demoralization, excessive fatigue, chronic malaise, moral ambivalence, sleep deprivation, and major depression, each introduced by these miniature mental munitions. Although these psychological impairments are singularly significant, they could also be additive, magnifying their bewildering effects.

Another targeting tool might be an ordinance that destroys trust while boosting paranoia, which could lead to emotional turmoil. Such behavior would sow dissent among operators and teams. Emotionally unstable, irrational, impaired warfighters directly reduce combat effectiveness and alter the chances of mission success. Because multiple individuals could be affected simultaneously or in synchrony, activating these futuristic weapons might trigger panic, fear, and violence in people and places far removed from defined war zones.

Far beyond shaping minds, the terrorism of tomorrow encompasses an all-out assault on physical and mental processes, affecting performance and perception. Those hit by nanoweapons might remain oblivious to their condition, worsening the situation. Like naive zombies, transformed soldiers may not exhibit overt, physical detriments and may continue to trudge through life, executing maladaptive actions. Understanding the far-reaching, incapacitating implications of weapons of this magnitude that target brain functions is essential for devising effective counterstrategies to deal with such a dangerous menace.

Universality of Threat

From manipulating cellular processes to disrupting ecological equilibriums, nanoweapons can unleash chaos across diverse biological systems, posing a threat to all living things, not just humans. Remarkably (and perhaps, unfortunately), humans share more than half their genes with other life-forms, spanning plants, insects, and animals. Dr. Robert H. Whittaker is credited with successfully organizing the living world into five kingdoms: the monera (blue-green algae), protists (phytoplankton), fungi (mushrooms), plants, and animals (including humans).[17] Surprisingly, humans even share 60 percent of our genes with bananas. Because the living world's genetic coding overlaps with that of humans, unwittingly, all species on the planet are now vulnerable to direct and indirect threats and destruction.

The living world is a complex network of interconnected organisms that metabolize, reproduce, and respond to environmental cues. Called "eukaryotes," life-forms whose nuclei have DNA inside comprise all animals and plants. Not all life-forms package information so neatly, and those with DNA without a nucleus inside their bodies are called "prokaryotes." Both eukaryotes and prokaryotes are essential contributors to the balance of nature and necessary to the survival and propagation of the human species. Nanoweapons targeting nonhuman DNA could selectively seek, disrupt, and destroy critical species across the globe with profound impacts.

Damaging the food chain or soil food web would produce devastation beyond imagination, quickly creating a downstream effect of food shortages becoming a horrific weapon.

Covertly introduced, weaponized intrusions' impacts on lower levels of the food chain could gradually reach unsuspecting targets months or even years after the munition's insertion. The far-reaching consequences of this all-encompassing indirect-targeting capability necessitate the thorough evaluation of delayed-effect defense strategies.

Nanoweaponry's potential to disrupt ecosystems, food and soil webs, and the ecological balance emphasizes the need for a renewed focus on environmental protection. Biodiversity conservation, ecosystem resilience, and sustainable development also must become central to future strategies to mitigate the far-reaching consequences of nanoweaponry. Like fields strewn with unexploded mines, the battlefields of tomorrow are tainted by nanoweaponry and could hold treacherous consequences for generations to come. Although environmental protection efforts traditionally focus on natural resources, habitat restoration, and pollution reduction, the advent of nanobased spoilage and its potential for irreparable damage necessitates a stronger emphasis on preventing harm and safeguarding the integrity of both local and global environments.

Mitigation Strategies and Challenges

Nanoweaponry's minuscule size, invisibility, and expansive living targets as well as the sheer complexity of molecular machinery make mitigation a formidable challenge. Despite this overwhelming task, several actions can be instituted or developed to detect and defuse munitions. Scientists must create genomic-level technologies that reverse

TOC

and recover humans' physical and mental health, heal all living creatures, and restore any damage done to the environment. Innovators must also develop nanoabilities to seek and depose those who would threaten terroristic action or actively deploy nanosized weapons of destruction.

Despite the unprecedented emerging threats from nanomunitions, their consequences are foreseeable, even if their actions are unseeable. Researchers must focus on developing nanoscale DNA-intrusion detectors and genomic-repair robots to prepare for conflicts on tomorrow's nanosized or picosized battlefields. Fortunately, the innovations that are used to create powerful weapons can also be used to prevent, detect, repair, and restore injuries inflicted by the weapons. Mitigation strategies are organized and discussed under store, monitor, alert, learn, and legislate groupings (SMALL). Although several of these technological mitigation strategies depend upon further innovation, we can immediately begin implementing the first and last categories. We can also start by creating formal connections with global leaders responsible for the protection of each living kingdom while formulating a research plan for the remaining capability gaps.

Store

Acquiring and storing all civilian and military-member DNA codes in a globally interconnected repository that is impeccably protected from unauthorized intrusions is imperative. Any service member starting duty has his or her DNA sample taken and stored; the current inventory contains more than nine million samples.[18] These samples have not been sequenced; their sole purpose is to confirm the identities of the deceased. Several commercial ventures, including 23andMe, which has over 12.8 million customers, provide hundreds of millions of customer results that can be accessed by China's WuXi Healthcare Ventures and others outside the United States.[19] The United States must protect this personally identifiable information and expand sequencing immediately to include everyone in the military and civilian populations. Then, the comprehensive database search engines can query and compare patterns to detect genomic intrusions and anomalies. Artificial intelligence and machine-learning algorithms that run on quantum systems can identify individual code changes and search across populations to identify unnatural sequences.

Additionally, we must extend the repository beyond humans and query and store DNA from all earthly inhabitants, whether they swim, grow, fly, graze, or simply exist; indeed, the compilation of this genetic data is the goal of the Earth BioGenome Project.[20] Like a genomic Noah's ark, this significant initiative focuses on sequencing and analyzing the genomes of all known eukaryotic species. The project—which aims to build a comprehensive digital library of Earth's life, thereby facilitating future discoveries—should be resourced heavily and prioritized.

Monitor

Once the reference codes of all living things are known and accessible, innovators should promote the development of digital epigenetic twins capable of monitoring daily fluctuations in patterns. This copy of oneself provides a reference source so that measuring changes and resetting the body and mind are possible. Methylation is an internal cellular process by which the human body regulates replication. Molecular locks open and hide portions of the DNA strand, affecting whether the strand is used for copying or left dormant. Nanosensors must be designed to detect subtle DNA changes, including mutations and repairs, while real-time epigenetic methylation monitors further enhance oversight and restoration.

A nano-NATO data-curation system with a dashboard would need to be created to assess and monitor complex situations across the globe. The system would have to sift through enormous amounts of human, animal, and plant data to look for early trends or isolated dangers. Indeed, the fidelity of the information from the vast networks of sensors is critical to ensuring actionable efforts. Static, inorganic nanosensors, which are suited for monitoring air, land, and water, can provide gross data on movements, contacts, and transfers. Organic, living nanosensors would be even more valuable in monitoring the living kingdoms. These nanosensors would be able to enter the cells of bodies and structures and be incorporated into diverse life-forms, including plants, insects, birds, and fish. These novel sensors could provide sustained standard communications across lifetimes and generations to report terroristic intrusions, ecosystem damage, or targeted attacks.

Alert

Developing nanorecovery agents that are capable of alerting and resetting fraudulent DNA and epigenetic changes is pivotal. Finding a suitable method will be difficult because of the dynamic nature of natural, epigenetic, protective changes as well as deleterious actions continuously occurring across the cells of human bodies and beyond. Humans only differ by 0.1 percent across the genome, so we are remarkably similarly constructed.[21]

One novel method might use the concept of jumping-gene mimicry, wherein genetic repeats act as decoys for mutagenic changes. Co-opting this natural process could be a promising, proactive method. Jumping genes could be programmed to move along DNA strands continuously, adhering and offering themselves to munitions for connection. Once bound, the section can be cleaved, resetting codes to preset levels and leaving the protected strand intact. Transposons, or jumping genes, can switch replication on and off and offer possibilities for recognizing malicious insertions and intrusions.[22]

Learn

Proactive tools, such as nanobot code sniffers, could search out targets, such as known terrorists or substate actors, using their unique genetic codes. Code sniffers could treat targets with several solutions, including identification, modification, or nullification. These microscopic security systems would bypass traditional identification methods, superseding biometrics and all other visual-confirmation techniques. Nanobot code sniffers could autonomously report the exact contact time and the results of the operation.

Future developments might allow the remote determination of genetic code, either through direct findings or indirectly through relatives and family extrapolations. Those who live or work closely together might be identifiable by shared environmental and personal traces of genomic material. Natural, inanimate, nanosized sensors could be dispersed across the living kingdoms and programmed to discover and document the DNA of inhabitants and those migrating through defined areas.

Legislate

Stringent regulations and treaties for verifiable compliance must be established, considering the historical challenges posed by technological advancements with military applications. Unique concerns arise over nanoweapons' effects, necessitating thorough deliberation, potential moratoriums, or outright bans of specific usages.

Unified agencies must craft cooperative agreements for humanity-crushing technologies like nanoweaponry and artificial, generalized intelligence. The task ahead is daunting due to the uncooperative nature of competing nations as well as terrorist actors who may be bolstered by the incredible power of these weapons. Essential for responding to breaches of standards, an integrated deterrence program requires a united, global response.

Conclusion

As we adapt to the rise of nanotechnology and its weaponization, safeguarding our DNA and genetic information is paramount. Nanoweaponry will significantly impact pacing challenges, and terrorists will undoubtedly position themselves to exploit any vulnerabilities. Because nanoweapons target individuals, nations, and the environment, they provoke fear and pose catastrophic environmental challenges that threaten global vitality.

To address this menace, we must develop defenses for our bodies and minds, devise methods of detecting covert activities, support innovations in healing and genomic restoration, and establish international alliances that deter evil forces from obtaining and employing these potent weapons. The incredible biological marvels within the genomes of millions of Earth's organisms are now at risk as those seeking power and dominance set their sights on the genomes. We are, in essence, the battleground of the future.

In Dr. Richard Feynman's lecture, "There's Plenty of Room at the Bottom," he predicted the development of miniaturized manufacturing, which he said would start larger and lead to building smaller and smaller machines by "maneuvering things atom by atom."[23] With discussion already past the nanometer level and heading toward the atomic level, futurists will use Feynman's process to direct research and development down to the picometer, which measures at the atomic level. By understanding the potential of picometer-sized science, we can begin to prepare for the next phase in the resolution revolution, perhaps reaching an understanding of particles so small they furnish the forces that separate living matter from nothingness. Weapons at the quantum level, which pose threats that far exceed those of our daily lives, could be used for interstellar wars in the future.[24]

Nanoweapons, which are characterized by their scalability, accessibility, directed control, and relative affordability, have the potential to alter ecosystems and human systems, making nanoweapons among the most dangerous threats we face today.

Although several authors have produced excellent work on nanotechnology and its weaponization, the work focuses mainly on the enabling side of nanotechnology, including soldier battle suits, enhanced materials, improved communication devices, and mininukes.[25] These developments are necessary and important, yet nanoweapons that target the intranuclear world of the cells of living things should be prioritized.

The magnitude of the dangers nanoweaponry poses may be overwhelming to many, and when confronted with the unimaginable, a typical coping response is avoidance. When dealing with something shocking, being in denial can provide time and space. Unfortunately, the peace-loving world does not have the luxury of either. If strategic leaders relegate this potentially cataclysmic technology to farcical fantasy or believe nanoweaponry is an ultraexpensive, impractical tool unworthy of concern, then these leaders will only amplify the danger.

Nanoweaponry is a threat to our present and our future. Nanotechnology is already being used in many weapons today.[26] Nanolasers, which generate intense light, are small, fast, powerful, and useful in missile and unmanned aerial defense systems. Aluminum-based nanochemicals are used in fuel cells, paints, coatings, and fabrics. These compounds are toxic and, if weaponized, could disrupt and kill living cells across the natural universe. Nanocatalysts are used in chemical processes and beneficial to living-organismal processes. These catalysts make batteries, waste-disposal systems, and sensors more efficient, which is a requirement for powered military efforts. Finally, nanoelectronics, which support communications, are used to create tiny robots tuned to deliver products, repair damage, or destroy specific targets.

The expense and complexities of biotechnology have been a traditional barrier to non-state actors that are able to create customized nanoweapons. Historically, non-state actors rarely used cutting-edge technology, relying instead on commercially available products.[27] A nanoid robot capable of light activation with specific cellular-targeting capability costs an estimated $100,000.[28] With scalable manufacturing, the cost could be reduced to just a few hundred dollars in a few years. Because the potentially damaging effects of nanoweaponry are high and its price is soon to be low, terrorists and non-state actors are much more likely to acquire and deploy these globe-altering munitions, breaking the tradition of avoidance.

Today, the threat of nanoweapons is real. Strategic planners and leaders must immediately create programs of education and protection and products for mitigation and restoration. The planners must fund further research, foster development, legislate, and regulate. Although nanotechnology in medicine may offer immortality, nanoweapons used by malevolent actors pose an existential threat to all living things. Although the dangers to humanity are becoming increasingly less visible, our collective actions and cooperative resolve must not be.

Endnotes

1. Andrew Kirima, “Macro Things Have Nano Beginnings,” DataDrivenInvestor (website), March 9, 2021, https://www.datadriveninvestor.com/2021/03/09/macro-things-have-nano-beginnings/.

2. Harald Sack, “Ernst Ruska and the Electron Microscope,” *SciHi* (blog), March 9, 2019, http://scihi.org/ernst-ruska-electron-microscope/.

3. Kirima, “Macro Things.”

4. Ilan Davis, “The ‘Super-Resolution’ Revolution,” *Biochemical Society Transactions* 37 (October 2009): 1042–44, https://doi.org/10.1042%2FBST0371042.

5. Michael Tabb, Andrea Gawrylewski, and Jeffery DelViscio, “What Is CRISPR, and Why Is It So Important?,” *Scientific American* (website), June 22, 2021, https://www.scientificamerican.com/video/what-is-crispr-and-why-is-it-so-important/.

6. Jurgen Altmann and Mark A. Gubrud, “Risks from Military Uses of Nanotechnology – The Need for Technological Assessment and Preventive Control,” in *Nanotechnology – Revolutionary Opportunities and Societal Implications*, ed. M. C. Roco and R. Tomellini (Luxembourg: Office for the Official Publications of the European Communities, 2002).

7. Louis A. Del Monte, *Nanoweapons: A Growing Threat to Humanity* (Lincoln, NE: Potomac Books, 2017).

8. Michael M. Crow and Daniel Sarewitz, “Nanotechnology and Societal Transformation,” in *American Association for the Advancement of Science Science and Technology Policy Yearbook 2001*, ed. Albert H. Teich and Stephen D. Nelson (Washington, DC: American Association for the Advancement of Science, 2001).

9. Jacopo Prisco, “Will Nanotechnology Soon Allow You to ‘Swallow the Doctor’?,” *CNN Business* (website), January 30, 2015, https://www.cnn.com/2015/01/29/tech/mci-nanobots-eth/index.html.

10. Alexey Kharlamov et al., “Nanothreats and Nanotoxicological Peculiarities of Nanoobjects as One of the Future Trends of Terrorist Threat,” in *Trends and Developments in Contemporary Terrorism*, ed. Dan-Radu Voica (Amsterdam: IOS Press, 2012), 33–47.

11. Debnath Bhattacharyya et al., “Nanotechnology, Big Things from a Tiny World: A Review,” *International Journal of u- and e- Service, Science and Technology* 2, no. 3 (September 2009).

12. “Duck and Cover, Civil Defense Pamphlet,” Oregon History Project (website), n.d., accessed on December 26, 2023, https://www.oregonhistoryproject.org/articles/historical-records/duck-and-cover-civil-defense-pamphlet/.

13. A. J. Marian, “Sequencing Your Genome: What Does It Mean?,” *Methodist DeBakey Cardiovascular Journal* 10, no. 1 (January-March 2014): 3–6, https://doi.org/10.14797%2Fmdcj-10-1-3.

14. Jenny Holzer, *Untitled (Fear Is the Most Elegant Weapon . . .), from Inflammatory Essays*, 1982, offset lithograph in black on yellow wove paper, 21 3/8 × 21 3/8” (54.2 × 54.2 cm), Art Institute Chicago, https://www.artic.edu/artworks/151321/untitled-fear-is-the-most-elegant-weapon-from-inflammatory-essays.

15. Di Wu et al., “The Blood-Brain Barrier: Structure, Regulation, and Drug Delivery,” *Signal Transduction and Targeted Therapy* 8, no. 1 (May 2023): 217ff, https://doi.org/10.1038/s41392-023-01481-w.

16. Jayesh B. Shah, “The History of Wound Care,” *Journal of the American College of Clinical Wound Specialists* 3, no. 3 (September 2011): 65–66, https://doi.org/10.1016/j.jcws.2012.04.002.

17. W. E. Westman and R. K. Peet, “Robert H. Whittaker (1920–1980): The Man and His Work,” in *Plant Community Ecology: Papers in Honor of Robert H. Whittaker*, ed. R. K. Peet (Berlin: Springer Dordrecht, 1985).

18. Alexandra Minor, “AFRSSIR [Armed Forces Repository of Specimen Samples for the Identification of Remains] Processes Nine Millionth DNA Reference Card,” Defense Visual Information Distribution Service (website), October 17, 2023, https://www.dvidshub.net/news/456210/afrssir-processes-9-millionth-dna-reference-card.

19. 23andMe, *23andMe Reports FY 2022 Fourth Quarter and Full Year Financial Results* (Sunnyvale, CA: 23andMe, May 25, 2022); and "WuXi Healthcare Invests in US Genomics Testmaker 23andMe," BioSpace (website), October 21, 2015, https://www.biospace.com/article/releases/-b-wuxi-healthcare-b-invests-in-us-genomics-testmaker-23andme-/.

20. Harris A. Lewin et al., "Earth BioGenome Project: Sequencing Life for the Future of Life," *Periodical of the National Academy of Sciences* 115, no. 17 (April 2018): 4325–33, https://doi.org/10.1073/pnas.1720115115.

21. "Human Origins: What Does It Mean to Be Human?," Smithsonian Museum of Natural History (website), n.d., accessed on December 26, 2023, https://naturalhistory.si.edu/education/school-programs/grades-6-12/human-origins-what-does-it-mean-be-human.

22. Sandeep Ravindran, "Barbara McClintock and the Discovery of Jumping Genes," *Periodical of the National Academy of Sciences* 109, no. 50 (December 2012): 20198–99, https://doi.org/10.1073%2Fpnas.1219372109.

23. Richard P. Feynman, "There's Plenty of Room at the Bottom," *Engineering and Science* 23, no. 5 (1960).

24. Ethan Siegel, "Is Humanity About to Accidentally Declare Interstellar War on Alien Civilizations?," *Forbes* (website), August 7, 2018, https://www.forbes.com/sites/startswithabang/2018/08/07/is-humanity-about-to-accidentally-declare-interstellar-war-on-alien-civilizations/?sh=3010c54926a9.

25. Patrick Tucker, "US Military Eyes New Mini-Nukes for 21st-Century Deterrence," *Defense One* (website), August 3, 2017, https://www.defenseone.com/technology/2017/08/us-military-eyes-new-mini-nukes-21st-century-deterrence/139997/.

26. Louis Del Monte, "Are Nanoweapons Paving the Road to Human Extinction?," *Huffington Post* (website), June 3, 2017, https://www.huffpost.com/entry/are-nanoweapons-paving-the-road-to-human-extinction_b_59332a52e4b00573ab57a3fe.

27. T. X. Hammes, "Technology Converges; Non-State Actors Benefit," Hoover Institution (website), February 25, 2019, https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

28. Murad, "Does Nanobots Exist – Are Nanobots Real," Sci Quest (website), n.d., accessed on December 26, 2023, https://sciquest.org/does-nanobots-exist/.

– 7 –

Conclusion

Paul J. Milas

The NATO Centre of Excellence Defence Against Terrorism (COE-DAT) emerging threats in terrorism project provides an urgent call to action in an evolving landscape where emerging technologies have become powerful instruments for non-state actors with malicious intent. The findings from the collaborative workshops held between NATO COE-DAT and the US Army War College Strategic Studies Institute highlight the potential threats stemming from the weaponization of artificial intelligence (AI), nanotechnology, augmented reality, and other cutting-edge advancements.

As NATO navigates the complex terrain of the future, the report draws attention to a sobering reality. Although recent advances in AI and autonomous systems hold the promise of early threat detection, terrorist groups are already exploiting them. The convergence of futurists' promises, ranging from the omnipresence of AI to the potential manipulation of human genes and the fusion of digital and physical worlds, intensifies the urgency to assess how these technologies might reshape the terrorist landscape in the next five to 10 years.

The report's focus on North America and South America highlights specific threats—from the malicious use of AI tools in recruitment and warfare to the potential leveraging of agricultural advancements for catastrophic attacks. The accessibility of emerging technologies, coupled with the democratizing effect they have, allows even small extremist cells to carry out mass-casualty attacks and pose a challenge to traditional counterterrorism efforts.

Forecasted scenarios involving AI, automated vehicles, augmented reality, and nanotechnology reveal potential threats ranging from deepfake disinformation videos to nanoweapons with precision targeting capabilities. The thinning line between fiction and reality, exemplified by scenarios seemingly drawn from Hollywood movies, underscores the transformative power of emerging technologies and the imperative to stay ahead of their potential malevolent applications.

The multifaceted recommendations for NATO include promoting international collaboration, supporting the development of ethical frameworks, and engineering safeguards into specific technology areas. This report advocates for a proactive approach to collaboration between scientists, innovators, and threat specialists and highlights the importance of anticipating and mitigating emerging threats.

With NATO and its Allies and partner nations standing at the intersection of geopolitical competition and technological advancements, the report calls for innovation, collective strength, international cooperation, and the acknowledgment that while terrorism response remains primarily a national responsibility, its success requires a global effort. The challenges posed by the weaponization of frontier technology demand a united front, where NATO's expertise and competence play a pivotal role in countering emerging threats and shaping a secure future.

About the Editors

Susan Sim is vice president for Asia of The Soufan Group, a global intelligence and security consultancy, and a senior research fellow with The Soufan Center, an independent, nonprofit organization that offers research, analysis, and strategic dialogue on global security challenges and foreign policy issues. Her publications include The Soufan Center's *Terrorism and Counterterrorism in Southeast Asia: Emerging Trends and Dynamics* (2021); chapters in *Good Practices in Counter Terrorism* (NATO Centre of Excellence Defence Against Terrorism, 2021); *The Routledge Handbook of Asian Security Studies*, 2nd ed. (Routledge, 2018); and *Homeland Security and Terrorism* (McGraw-Hill, 2013). Sim is also an adjunct senior fellow at the S. Rajaratnam School of International Studies and the editor of the *Home Team Journal*, the flagship publication of the Singapore Ministry of Home Affairs.

Colonel Eric Hartunian, US Army, PhD, is an Army strategist and the director of strategic research and analysis at the Strategic Studies Institute at the US Army War College, where he supervises researchers studying regional and functional topics of import to the defense community. He has served in leadership positions across the Army, with deployments to Iraq and Afghanistan. Hartunian was the chief strategist at the National Counterterrorism Center's Directorate of Strategic and Operational Planning, where he focused on counterterrorism policy to include the global foreign fighter crisis and other counter-ISIS challenges. He holds a PhD in public administration from the University of Kansas and a master's degree in defense analysis from the Naval Postgraduate School. He is also a fellow with the US Army's Advanced Strategic Planning and Policy Program.

Lieutenant Colonel Paul J. Milas, US Army, is the director of African affairs at the Strategic Studies Institute at the US Army War College. He holds a master of international public policy degree from Johns Hopkins University and a bachelor of arts in political science from Indiana University.

TOC

About the Contributors

Darrin L. Frye, MD, MPH, is the associate professor of science and technology and innovative futures and the head of the Department of Strategic Intelligence and Emergent Technologies at Joint Special Operations University at MacDill Air Force Base in Tampa, Florida. Frye possesses three decades of clinical experience in surgical, emergency, preventive, and performance medicine in addition to his medical military soldier career. Currently, at Joint Special Operations University, Frye focuses on teaching and learning, research and analysis, and service and outreach related to emerging technologies that are critical for the success of the special operations enterprise. Frye's educational background includes a medical doctorate from the University of Kansas School of Medicine, a master of public health from Florida International University, and a bachelor of general studies in human biology from the University of Kansas.

Sarah Lohmann, PhD, is a member of the full-time teaching faculty at the Information School at the University of Washington. Lohmann's research and instruction focus on information technology governance, cybersecurity, and emerging and energy technologies. Lohmann is also an author and editor of two recent books: *What Ukraine Taught NATO about Hybrid Warfare* (US Army War College Press, 2022) and *Countering Terrorism on Tomorrow's Battlefield* (US Army War College Press, 2022). Lohmann holds a doctorate in political science from the Universität der Bundeswehr München.

Michael W. Parrott serves as the Special Operations Forces Counterintelligence Integration Course director at the Joint Special Operations University, MacDill Air Force Base, Florida. He is responsible for the development, execution, and instruction of Joint Force Special Operations Forces curriculum. Parrott is a highly effective and dynamically accomplished former special operations intelligence management professional. He holds a master of arts degree in strategic security studies from the College of International Security Affairs at the National Defense University, a bachelor of arts in homeland security with a concentration in terrorism studies from the American Military University, and an associate of applied science degree in intelligence operations.

Steve Sin, PhD, is an assistant research scientist and the director of the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism. He develops, leads, and manages interdisciplinary research projects that span a broad range of national and homeland-security challenges. Sin's expertise includes countering weapons of mass destruction, operations in the information environment, asymmetric threat and irregular warfare, and northeast Asian regional security. He holds a PhD in political science from the University at Albany, State University of New York, and is fluent in Korean, Mandarin Chinese, and Japanese.

Kristan J. Wheaton is the professor of strategic futures at the US Army War College, where he teaches the Futures Seminar. Designed to help Army senior leaders think more rigorously and effectively under conditions of deep uncertainty, the Futures Seminar is a six-month, project-based program that looks at political, technical, business, and social trends that could impact the Army. Wheaton also manages the Futures Lab, which exposes senior Army leaders to cutting-edge commercial technologies. He is the author of the *Sources and Methods* blog and several books, including *The Warning Solution: Intelligent Analysis in the Age of Information Overload* (AFCEA International, 2001), and *Wikis and Intelligence Analysis* (2012).

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers in the global application of Landpower. Concurrently, it is our duty to the Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate on the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The SSI Live Podcast Series provides access to SSI analyses and scholars on issues related to national security and military strategy with an emphasis on geostrategic analysis.

The Center for Strategic Leadership provides strategic education, ideas, doctrine, and capabilities to the Army, the Joint Force, and the nation. The Army, Joint Force, and national partners recognize the Center for Strategic Leadership as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.

The School of Strategic Landpower provides support to the US Army War College purpose, mission, vision, and the academic teaching departments through theinitiation, coordination, and management of academic-related policy, plans, programs, and procedures, with emphasis on curriculum development, execution, and evaluation; planning and execution of independent and/or interdepartmental academic programs; student and faculty development; and performance of academic-related functions as may be directed by the commandant.

The US Army Heritage and Education Center engages, inspires, and informs the Army, the American people, and global partners with a unique and enduring source of knowledge and thought.

The Army Strategic Education Program executes general officer professional military education for the entire population of Army general officers across the total force and provides assessments to keep senior leaders informed and to support programmatic change through evidence-based decision making.

USAWC PRESS

The US Army War College Press supports the US Army War College by publishing monographs and a quarterly academic journal, *Parameters*, focused on geostrategic issues, national security, and Landpower. Press materials are distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities. The US Army War College Press serves as a bridge to the wider strategic community.

All US Army Strategic Studies Institute and US Army War College Press publications and podcasts may be downloaded free of charge from the US Army War College website. Hard copies of certain publications may also be obtained through the US Government Bookstore website at https://bookstore.gpo.gov. US Army Strategic Studies Institute and US Army War College publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the US Army Strategic Studies Institute and the US Army War College Press, US Army War College, Carlisle, PA. Contact the US Army Strategic Studies Institute or the US Army War College Press by visiting the websites at: https://ssi.armywarcollege.edu and https://press.armywarcollege.edu.

The US Army War College Press produces two podcast series. Decisive Point, the podcast companion series to the US Army War College Press, features authors discussing the research presented in their articles and publications. Visit the website at: https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Decisive-Point-Podcast/. Conversations on Strategy, a Decisive Point podcast subseries, features distinguished authors and contributors who explore timely issues in national security affairs. Visit the website at: https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Conversations-on-Strategy-Podcast/.

UNITED STATES ARMY
WAR COLLEGE

CENTRE OF
EXCELLENCE DEFENCE
AGAINST TERRORISM

US ARMY WAR COLLEGE

Commandant
Major General David C. Hill

STRATEGIC STUDIES INSTITUTE

Director
Dr. Carol V. Evans

Director, China Landpower Studies Center
Colonel Richard D. Butler

Director, Strategic Research and Analysis
Colonel Eric Hartunian

US ARMY WAR COLLEGE PRESS

Editor in Chief
Dr. Antulio J. Echevarria II

Digital Media Manager
Mr. Richard K. Leach

Managing Editor
Ms. Lori K. Janning

Developmental Editor
Dr. Erin M. Forest

Copy Editors
Ms. Stephanie Crider
Ms. Elizabeth Foster

Visual Information Specialists
Ms. Kaitlyn Guettler
Ms. Kristen G. Taylor

Composition
Mrs. Jennifer E. Nevil

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM (COE-DAT)

Director
Colonel Bülent Akdeniz (Türkiye)

Deputy Director
Colonel H. Warren Rohlfs (United States)

Project Managers
Lieutenant Colonel Uwe Berger (Germany)
Major Ali Mavuş (Türkiye)

U.S. ARMY

ISBN 1-58487-852-5
90000
9 781584 878520